UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)**	**Docket No. RM13-_____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF RETIREMENT OF REQUIREMENTS IN RELIABILITY STANDARDS

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

Counsel for the North American Electric Reliability Corporation

February 28, 2013

TABLE OF CONTENTS

EXHIBITS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)**	**Docket No. RM13-_____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF RETIREMENT OF REQUIREMENTS

The North American Electric Reliability Corporation ("NERC")[1] respectfully requests the Federal Energy Regulatory Commission ("FERC" or the "Commission") approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[2] and Section 39.5 of the Commission's Regulations, 18 C.F.R. § 39.5 (2012), the retirement of 34 requirements within 19 currently effective Reliability Standards as set forth in **Exhibit B**,[3] concurrent with the effective day of Commission approval.[4]

The following Regional Entities and organizations have authorized NERC to state that they support the filing of this petition: American Public Power Association, Canadian Electricity Association, Edison Electric Institute, Electricity Consumers Resource Council, Florida Reliability Coordinating Council, Large Public Power Coordinating Council, Midwest Reliability Organization, National Rural Electric Cooperative Association, Northeast Power

---

[1] NERC has been certified by the Commission as the electric reliability organization ("ERO") in accordance with Section 215 of the Federal Power Act. The Commission certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

[2] 16 U.S.C. § 824o (2012).

[3] Unless otherwise designated herein, all capitalized terms shall have the meaning set forth in the Glossary of Terms Used in NERC Reliability Standards, available here: http://www.nerc.com/files/Glossary_of_Terms.pdf.

[4] Note, for the purposes of this petition, the term "requirement" encompasses sub-requirements. The Violation Risk Factors ("VRFs) and Violation Severity Levels ("VSLs") for the requirements proposed for retirement would also be retired. Conforming changes were also made to VSLs of other requirements in these Reliability Standards that reference the requirements proposed for retirement. Note that upon Commission approval of the retirement of these requirements, the version numbers of the standards will not be incremented, but the retired requirements and associated elements will be clearly marked as "retired."

Coordinating Council, Reliability*First* Corporation, SERC Reliability Corporation, Southwest Power Pool Regional Entity, Texas Reliability Entity, Inc., Transmission Access Policy Study Group, and the Western Electricity Coordinating Council.

I. EXECUTIVE SUMMARY

Consistent with the Commission's order approving NERC's Compliance Enforcement Initiative ("CEI"), including the Find, Fix, Track and Report ("FFT") program, NERC is requesting retirement of 34 requirements within 19 Reliability Standards that are redundant or otherwise unnecessary, and where violations of these requirements (currently included in Reliability Standards) pose a lesser risk to the reliability of the Bulk-Power System. No Reliability Standard is being proposed for retirement in its entirety, and all other requirements in each of the affected Reliability Standards will remain in continuous effect.

NERC's mission is to ensure and improve the reliability of the Bulk-Power System. Reliability excellence is achieved through the ongoing identification, correction and prevention of reliability risks, both big and small. Yet, accountability for reliability excellence is broader than just penalizing violations. NERC's CEI and, in particular the FFT program, represent a significant change in the paradigm for monitoring and enforcing compliance with Reliability Standards. The FFT program allows NERC and the Regional Entities flexibility to process and track lesser risk violations more efficiently in order to focus their resources on issues that pose the greatest risk to reliability. Consistent with this approach, NERC is proposing to retire requirements in Reliability Standards that can be removed with little to no effect on reliability. The retirement of these requirements will allow industry stakeholders to focus their resources appropriately on reliability risks and will increase the efficiency of the ERO compliance program.

A. Background

On March 15, 2012, the Commission issued an order[5] on the NERC FFT program that stated in paragraph 81 ("P 81"):

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. ***If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief***. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards ***unnecessary or redundant*** requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

In response to the Commission's FFT Order and, specifically, the language in P 81, a joint collaborative effort was formed among various industry stakeholders, trade associations,[6] NERC Staff, and Staff from the Regional Entities; this effort became known as "P 81."[7] The trade associations, NERC Staff, and Staff from the Regional Entities each independently developed a list of possible Reliability Standard requirements appropriate for retirement, consisting only of currently active and enforceable standards. Working together, and through a series of discussions, the P 81 Team developed a list of requirements that were presented to the Standards Committee in the form of a Standards Authorization Request ("SAR"). The P 81 project was a

---

[5] *North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 at P 81 (2012)(emphasis added)("FFT Order").

[6] Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association and Transmission Access Policy Study Group.

[7] **Exhibit G** contains a list of the Project 2013-02 team members ("P 81 Team").

collaborative effort in recognition of the Commission's request that NERC, the Regional Entities, and interested parties coordinate to submit any comments in response to the FFT Order concurrently.

The scope of the P 81 project was limited solely to the removal of requirements in their entirety that would not otherwise compromise the integrity of the specific Reliability Standard or impact the reliability of the BES. The criteria developed by the P 81 Team were designed so that no rewriting or consolidation of requirements would be necessary and are provided herein as **Exhibit A,** for informational purposes only. The P 81 Team developed three criteria: (1) Criteria A: an overarching criteria designed to determine that there is no reliability gap created by the proposed retirement; (2) Criteria B: consists of seven separate identifying criteria designed to recognize requirements appropriate for retirement (administrative; data collection/data retention; documentation; reporting; periodic updates; commercial or business practice; and redundant); and (3) Criteria C: consists of seven separate questions designed to assist the P 81 Team in making an informed decision regarding whether requirements are appropriate to propose for retirement.[8]

B. Paragraph 81 – Requirements Proposed for Retirement

NERC has over 150 mandatory and enforceable Reliability Standards that contain over 1,300 requirements. There are fourteen separate bodies of NERC Reliability Standards:

[8] C1: Was the Reliability Standard requirement part of a FFT filing?
C2: Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?
C3: What is the VRF of the Reliability Standard requirement?
C4: In which tier of the 2013 AML does the Reliability Standard requirement fall?
C5: Is there a possible negative impact on NERC's published and posted reliability principles?
C6: Is there any negative impact on the defense in depth protection of the Bulk Electric System?
C7: Does the retirement promote results or performance based Reliability Standards?

(1) Resource and Demand Balancing ("BAL");

(2) Communications ("COM");

(3) Critical Infrastructure Protection ("CIP");

(4) Emergency Preparedness and Operations ("EOP");

(5) Facilities Design, Connections, and Maintenance ("FAC");

(6) Interchange Scheduling and Coordination ("INT");

(7) Interconnection Reliability Operations and Coordination ("IRO");

(8) Modeling, Data, and Analysis ("MOD");

(9) Nuclear ("NUC");

(10) Personnel Performance, Training, and Qualifications ("PER");

(11) Protection and Control ("PRC");

(12) Transmission Operations ("TOP");

(13) Transmission Planning ("TPL"); and

(14) Voltage and Reactive ("VAR").

Requirements from nine of these bodies of Reliability Standards are proposed for retirement; no requirements from COM, MOD, PER, TOP, or TPL Reliability Standards are included. Consistent with the Commission's guidance in the FFT Order, NERC proposes to retire the following "unnecessary or redundant requirements."[9]

[9] FFT Order at P 81.

Requirements Proposed for Retirement[10]		
BAL-005-0.2b R2	CIP-003-4 R4.2	INT-007-1 R1.2
CIP-003-3 R1.2	CIP-005-3a R2.6	IRO-016-1 R2
CIP-003-3 R3	CIP-005-4a R2.6	NUC-001-2 R9.1
CIP-003-3 R3.1	CIP-007-3 R7.3	NUC-001-2 R9.1.1
CIP-003-3 R3.2	CIP-007-4 R7.3	NUC-001-2 R9.1.2
CIP-003-3 R3.3	EOP-005-2 R3.1	NUC-001-2 R9.1.3
CIP-003-3 R4.2	FAC-002-1 R2	NUC-001-2 R9.1.4
CIP-003-4 R1.2	FAC-008-3 R4	PRC-010-0 R2
CIP-003-4 R3	FAC-008-3 R5	PRC-022-1 R2
CIP-003-4 R3.1	FAC-010-2.1 R5	VAR-001-2 R5
CIP-003-4 R3.2	FAC-011-2 R5	
CIP-003-4 R3.3	FAC-013-2 R3	

Just as the Commission regularly reviews its regulations to ensure that they achieve their intended purpose and do not impose an undue burden or unnecessary costs,[11] it is appropriate for NERC to evaluate its Reliability Standards in the same light. It is important to recognize that the regime of mandatory Reliability Standards is only seven years old. On April 4, 2006, as modified on August 28, 2006, NERC submitted to the Commission a petition seeking approval

[10] FAC-008-1 Requirements R2 and R3 are not included herein as they are no longer in effect. FAC-008-1 was superseded by FAC-008-3 on December 31, 2012.

[11] Written Testimony of Chairman Jon Wellinghoff before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, July 7, 2011, at p. 2 ("The Commission regularly reviews its regulations to ensure that they achieve their intended purpose and do not impose undue burdens on regulated entities or unnecessary costs on those entities or their customers."). Subsequently, on July 11, 2011, President Barack Obama issued an Executive Order to independent agencies, such as FERC, to develop and release a plan to review rules that may be outmoded, ineffective, insufficient, or excessively burdensome, and to modify, streamline, expand, or repeal them in accordance with what has been learned. President Barack Obama's Executive Order 13579, Regulation and Independent Regulatory Agencies at Section 2 (July 11, 2011). Chairman Jon Wellinghoff announced that same day that the Commission would implement President Barack Obama's Executive Order. FERC News Release, "FERC To Institute Public Review of Regulations" (July 11, 2011).

of 107 proposed Reliability Standards. Since that time, both NERC and the Commission have evolved and refined their respective approaches to what constitutes a Reliability Standard, and the P 81 project is illustrative of this maturation.

The ERO compliance program and stakeholders will benefit from the proposed retirement of the requirements included herein as efforts will appropriately be directed towards activities with a greater potential impact on reliability – these benefits translate into time and resources saved, which helps ensure that the costs of reliability are proportionate to the benefits.

The recent Petition for Approval of the CIP Version 5 Reliability Standards in Docket No. RM13-5-000, proposes to "eliminate unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System"[12] and is consistent with the principles of the P 81 Project and the Commission's language in Paragraph 81.

The primary focus of the P 81 Team was on retiring those lower-level facilitating requirements that are either redundant with other requirements or where evidence retention is burdensome and the requirement is unnecessary (*e.g.*, the same performance is addressed through other enforceable standards or mechanisms). NERC has authority to enforce reporting obligations pursuant to the Rules of Procedure.[13] Section 400 and Appendix 4C of the Rules of Procedure also set forth how failure to comply with a reporting obligation will be addressed. In the event a registered entity does not submit requested data, information, or a report, the registered entity is afforded several opportunities to respond or cure a request or requirement

[12] Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection Reliability Standards Version 5, Docket No. RM13-5-000 at 5 (January 31, 2013).

[13] Section 401.3 of the NERC Rules of Procedure provides that NERC and the Regional Entities can require "[a]ll Bulk Power System owners, operators and users" to provide "such information as is necessary to monitor compliance with the reliability standards." Appendix 4C to the NERC Rules of Procedure states that the Compliance Enforcement Authority will "*monitor, assess, and enforce* compliance with Reliability Standards using the compliance monitoring processes. . .to collect information in order to make assessments of compliance." Section 3.0 (emphasis added).

pursuant to Attachment 1 to Appendix 4C.[14] In December 2012, the Commission found that Attachment 1 to Appendix 4C "provides reasonable, measured and lawful responses to entities that are non-responsive to requests for data."[15]

Commission regulations further provide that all users, owners and operators of the Bulk-Power System "subject to the Commission's reliability jurisdiction. . .shall comply with applicable Reliability Standards, the Commission's regulations, and applicable Electric Reliability Organization. . .Rules made effective under this part."[16] The regulations also provide that "[e]ach user, owner or operator of the Bulk-Power System within the United States. . .shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization. . . ."[17]

Therefore, the proposed retirement of the documentation requirements included herein does not create a gap in reliability as NERC and the Regional Entities can enforce reporting obligations pursuant to section 400 of NERC's Rules of Procedure and Appendix 4C to ensure that necessary data continues to be submitted for compliance and enforcement purposes. Further, data necessary for NERC to implement Section 215 of the FPA can be obtained pursuant to Section 1600 of the NERC Rules of Procedure.[18]

---

[14] Attachment 1 to Appendix 4C to the CMEP: Process for Non-Submittal of Requested Data, Steps 1-3.

[15] ROP Order at P 82.

[16] 18 C.F.R. 39.2(b) (2012).

[17] 18 C.F.R. 39.2(d) (2012); *see also* Attachment 1 to Appendix 4C to the NERC Rules of Procedure.

[18] In Order No. 672, the Commission set forth the legal basis for Section 1600 of the NERC Rules of Procedure in creating Section 39.2 of the Commission's regulations. 18 C.F.R. § 39.2 provides:

> (d) Each user, owner or operator of the Bulk-Power System within the United States (other than Alaska and Hawaii) shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization and each applicable

While the P 81 Project proposes to retire several requirements related to data retention or documentation, NERC notes that the simple fact that a requirement includes a data retention or documentation element **does not** signify that it should be considered for retirement or is otherwise inappropriately designated as a requirement. Indeed, certain data retention and/or documentation requirements are essential to reliability.

As explained in the 2013-2015 NERC Reliability Standards Development Plan,[19] concepts from the P 81 Project will be carried forward into improving the future drafting of Reliability Standards. Projects will involve stronger examination for duplication of requirements across the NERC body of Reliability Standards and the technical basis and necessity for each and every requirement will continue to be evaluated. Specifically, the 2013-2015 NERC Reliability Standards Development Plan sets forth an aggressive schedule for 2013 to review Reliability Standards while applying P 81 and results-based concepts across the following three major work areas:

- **Existing Projects/Emerging Issues** - Current projects must be completed and new projects that either support high risk reliability issues or emerging issues must be conducted in a timely and efficient manner.
- **Reviews** - Five-year reviews must be conducted on standards that are due for assessment and have not been revised in recent standards development projects.
- **Directives** - Commission directives must be addressed and the resulting revised standards filed.

Regional Entity. The Electric Reliability Organization and each Regional Entity shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act.

[19] Submitted in Docket Nos. RM05-17-000 et al. (December 31, 2012), available at: http://www.nerc.com/files/2013-2015_RSDP_2012.12.31_complete.pdf.

Requirements that were proposed and ultimately not included in Phase 1 of the P 81 Project will be mapped for consideration as Reliability Standards are evaluated as part of these major work areas. It is expected that as a result of these projects, NERC will enhance the quality of its Reliability Standards.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[20]

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco*****
Senior Vice President and General Counsel
Holly A. Hawkins*****
Assistant General Counsel
Stacey Tyrewala*****
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

III. REGULATORY BACKGROUND

By enacting the Energy Policy Act of 2005,[21] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215 of the

[20] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

[21] 16 U.S.C. § 824o (2012).

FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards.[22]

Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c)(1) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard. In Order No. 693, the Commission noted that it would defer to the "technical expertise" of the ERO with respect to the content of a Reliability Standard and explained that, through the use of directives, it provides guidance but does not dictate an outcome. Rather, the Commission will consider an equivalent alternative approach provided that the ERO demonstrates that the alternative will address the Commission's underlying concern or goal as efficiently and effectively as the Commission's proposal, example, or directive.[23]

Section 39.5(a) of the Commission's regulations requires the ERO to file with the Commission for its approval each Reliability Standard that the ERO proposes to become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to be made effective. The Commission has the regulatory responsibility to approve standards that protect the reliability of the Bulk-Power System and to ensure that such standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest.

[22] *See* Section 215(b)(1)("All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section.").

[23] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 at PP 31, 186-187, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

IV. REQUIREMENTS PROPOSED FOR RETIREMENT

Listed below are the requirements proposed for retirement, organized by each of the nine relevant bodies of Reliability Standards. Each requirement proposed for retirement includes the following: (a) the text of the requirement proposed for retirement; (b) the complete procedural history of the Reliability Standard; and (c) the technical justification to support the proposed retirement.

A. Resource and Demand Balancing Reliability Standards

One standard from the BAL body of Reliability Standards, BAL-005, contains a requirement proposed for retirement. Collectively, the six BAL Reliability Standards address balancing resources and demand to maintain interconnection frequency within prescribed limits.

1. BAL-005-0.2b, Requirement R2 – Automatic Generation Control

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

a. Procedural History

BAL-005-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[24] Also, the Commission accepted an errata filing to BAL-005-0.1b, which replaced Appendix 1 with a corrected version of a Commission-approved interpretation, and made an internal reference correction in the interpretation, thus resulting in BAL-005-0.2b.[25]

b. Technical Justification for Retirement

The stated reliability purpose of BAL-005-0.2b is to establish requirements for Balancing Authority Automatic Generation Control ("AGC") necessary to calculate Area Control Error

[24] Order No. 693 at P 420.

[25] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Errata Changes to Seven Reliability Standards, Docket No. RD12-4-000 (September 13, 2012).

("ACE") and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved. The reliability purpose and objectives of BAL-005-0.2b are unaffected by the proposed retirement of Requirement R2.

BAL-005-0.2b Requirement R2 involves two important concepts- AGC and Regulating Reserve. AGC is defined in the NERC Glossary of Terms Used in Reliability Standards as follows: "Equipment that automatically adjusts generation in a Balancing Authority Area from a central location to maintain the Balancing Authority's interchange schedule plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction." Regulating Reserve is defined as: "An amount of reserve responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin." Regulating Reserve provides the margin that allows generation to respond to changing load conditions based on its calculated Area Control Error provided by its Energy Management System. It is not intended to provide response for frequency excursions or generation unit trips.

BAL-005 is related to BAL-001 – Real Power Balancing Control Performance. A Balancing Authority must use AGC to control its Regulating Reserves to meet the Control Performance Standards ("CPS") as set forth in BAL-001-0.1a Requirements R1 and R2.[26] The primary purpose of Requirement R2 is to specify how a Balancing Authority must meet CPS, *i.e.* through the use of AGC.

[26] Note, (i) if a BA does not have an adequate amount of regulating margin (Regulating Reserve) it will not meet CPS consistently; (ii) the fact that a BA does not meet CPS does not mean it has inadequate regulating margin, but may be an indication of poor control or some other influence. A BA may have more than an adequate amount of regulating margin, but may not be utilizing it to optimize the CPS measures; and (iii) if a BA does not meet CPS, it also does not necessarily mean the BA is operating unreliably. CPS is a consistent measure within the industry, to achieve a uniformity of practice and provide equity amongst the BAs operating within a common electric system.

NERC acknowledges that an argument regarding the redundancy of BAL-005 Requirement R2 was previously rejected by the Commission,[27] however, NERC maintains that this Requirement is redundant in an operational sense. Although for a short period of time (as the Commission stated during an AGC malfunction)[28] a Balancing Authority may be able to meet its CPS obligations without AGC, it cannot do so for any extended period of time, and, therefore, Balancing Authorities must use AGC to control Regulating Reserves to satisfy obligations under BAL-001-0.1a Requirements R1 and R2. Given this fact, BAL-005-0.2b Requirement R2 is redundant and having two requirements requiring the same activity means that there is no reliability gap created by the proposed retirement of BAL-005-0.2b Requirement R2. In other words, without the existence of BAL-005-0.2b Requirement R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a Requirements R1 and R2.

B. Critical Infrastructure Protection Reliability Standards

Eight requirements in the CIP body of Reliability Standards are proposed for retirement, however, two *versions* of these requirements are proposed to be retired, bringing the total to sixteen. The recently filed petition for approval of Version 5 of the CIP Reliability Standards is consistent with the proposed retirement of these requirements as explained below.

1. CIP-003-3, -4, Requirement R1.2 – Cyber Security – Security Management Controls

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

---

[27] *North American Electric Reliability Corp.*, 121 FERC ¶ 61,179 at PP 48-51 (2007).

[28] *Id.* at P 50 ("While theoretically, CPS can be met without the use of AGC, for example, when the AGC system is malfunctioning…").

a. Procedural History

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[29] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[30] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[31] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[32]

b. Technical Justification for Retirement

CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. The reliability purpose and objectives of CIP-003 are unaffected by the proposed retirement of Requirement R1.2.

CIP-003 Requirement R1.2 is an administrative task that requires Responsible Entities to ensure that their cyber security policy is readily available to personnel. To implement CIP-003-3, -4 R1.2 entities have undertaken a variety of administrative solutions including: kiosks dedicated to computers with the cyber security policy; posting the policy on the company intranet; and having copies available in work stations, at common area desks in generating stations and substations, *etc*. The proposed retirement of CIP-003, Requirement R1.2 is consistent with reliability principles and will not create a gap in reliability. Further, this

---

[29] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[30] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

[31] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

[32] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

requirement has been removed from CIP Version 5, and, therefore, CIP Version 5 supports, and is consistent with, the proposed retirement of this requirement.

2. CIP-003-3, -4 Requirements R3, R3.1, R3.2, R3.3 – Cyber Security – Security Management Controls

R3. Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

a. Procedural History

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[33] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[34] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[35] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[36]

---

[33] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[34] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

[35] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

[36] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

b. Technical Justification for Retirement

CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. The reliability purpose and objectives of CIP-003 are unaffected by the proposed retirement of Requirements R3, and R3.1 through R3.3.

CIP-003-3, -4 Requirements R3, R3.1, R3.2, and R3.3 (collectively "CIP Exception Requirements") are administrative tasks and the proposed retirement of these requirements presents no reliability gap. The CIP Exception Requirements only apply to exceptions to internal corporate policy, and only in cases where the policy exceeds a Reliability Standard requirement or addresses an issue that is not covered in a Reliability Standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of eight characters in length, and be changed every 30 days, (which is beyond the minimum requirements in CIP-007-3 Requirement R5.3), the CIP Exception Requirements could be invoked for internal governance purposes to lessen the corporate requirement back to the password requirements in CIP-007-3 R5.3. However, under no circumstances do the CIP Exception Requirements authorize the implementation of security measures that are less than what is required in CIP-007-3 Requirement R5.3.

The proposed retirement of the CIP Exception Requirements would not impact an entity's ability to maintain such an exception process within its corporate policy governance procedures, if it so desired. Fundamentally, the CIP Exception Requirements are an administrative tool for internal corporate governance procedures, and, therefore the proposed retirement of these requirements presents no reliability gap. The CIP Exception Requirements have been removed from CIP Version 5, therefore, Version 5 is consistent with, and supports, the proposed retirement of these requirements.

3. CIP-003-3 -4, Requirement R4.2 – Cyber Security – Security Management Controls

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

a. Procedural History

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[37] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[38] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[39] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[40]

b. Technical Justification for Retirement

Both Versions 3 and 4 of CIP-003 Requirement R4.2 require Responsible Entities to classify information based on "sensitivity." The proposed retirement of this requirement is consistent with CIP Version 5. While CIP-003-4 Requirement R4.2 has been incorporated into CIP-011-5 Requirement R1.1, the obligation to classify information based on sensitivity has been removed, which does not prevent companies from having multiple levels of classification, but allows more flexibility to incorporate the CIP information protection program into the normal

---

[37] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

[38] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

[39] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

[40] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, (2012).

course of business. Therefore, Version 5 supports, and is consistent with, the proposed retirement of this requirement.

The task of classifying Critical Cyber Information "based on the sensitivity" is an administrative task that is redundant with CIP-003-3, -4 Requirement R4. Specifically, CIP-003-3, -4 Requirement R4 already requires the classification of information associated with Critical Cyber Assets. The only difference between Requirement R4 and R4.2 is that the subjective term "based on the sensitivity" has been added, thus, making it essentially redundant. Further, CIP-003-3, -4 Requirement R4 requires the entity to develop classifications based on a subjective understanding of sensitivity (*i.e.,* no clear connection to serving reliability), therefore the proposed retirement of this requirement presents no reliability gap.

4. CIP-005-3a, -4a, Requirement R2.6 – Cyber Security -- Electronic Security Perimeter(s)

R2.6. Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

a. Procedural History

CIP-005-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[41] CIP-005-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RD09-7-000 and RM06-22-000 and was approved on September 30, 2009.[42] CIP-005-2a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by unpublished letter order on February 2,

[41] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

[42] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

2011.[43] CIP-005-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[44] CIP-005-3a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by an unpublished letter order on February 2, 2011.[45] CIP-005-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No. 761.[46] CIP-005-4a was filed for Commission approval as errata to the CIP Version 4 Petition on April 12, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No 761, the Final Rule on the CIP Version 4 standards.[47]

b. Technical Justification for Retirement

The implementation of an appropriate use banner ("banner") on a user's screen for all interactive access attempts into the Electronic Security Perimeter ("ESP") is an activity or task that is administrative. As noted by the CIP Version 5 drafting team:

> The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.[48]

This Requirement has been removed from CIP Version 5, therefore Version 5 is consistent with, and supports, the proposed retirement of this requirement.

---

[43] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).

[44] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

[45] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).

[46] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

[47] *Id.*

[48] See Project 2008-06 - Cyber Security Order 706 - Version 5, Mapping Document, available here: http://www.nerc.com/docs/standards/sar/Mapping_Document_for_CIP_V5_Clean_(2012-0911).pdf.

The banner does not ensure a proper or secure access point configuration which is generally the purpose of CIP-005-3a, -4a. Further, this requirement has also been the subject of numerous technical feasibility exceptions (commonly referred to as "TFEs") for devices that cannot support such a banner, and hence has diverted resources from more productive efforts.[49] Thus, the ERO's compliance program would become more efficient if CIP-005-3a, -4a R2.6 was retired, because ERO time and resources could be reallocated to monitor compliance with the remainder of CIP-005-3a, -4a, which provides for more effective controls of electronic access at all electronic access points into the ESP. Accordingly, the proposed retirement of CIP-005-3a, -4a, Requirement R2.6 presents no reliability gap.

5. CIP-007-3, -4, Requirement R7.3 – Cyber Security – Systems Security Management

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

a. Procedural History

CIP-007-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[50] CIP-007-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[51] CIP-007-2a was filed for Commission approval on November 17, 2009 in Docket No. RD10-3-000 and was approved on March 18, 2010.[52] CIP-007-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and

[49] *See* 2012 Annual Report of the North American Electric Reliability Corporation on Wide-Area Analysis of Technical Feasibility Exceptions, Docket No. RR10-1-001 at 6 (September 28, 2012).

[50] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

[51] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

[52] Order Approving Reliability Standard Interpretation, 130 FERC ¶ 61,184 (2010).

was approved on March 31, 2010.[53] CIP-007-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[54]

b. Technical Justification for Retirement

CIP-007-3, -4 Requirement R7.3 requires the maintaining of records for the purpose of demonstrating compliance with disposing of or redeploying Cyber Assets in accordance with documented procedures. NERC and the Regional Entities, however, under Section 400 of the NERC Rules of Procedure, have the ability to require the production of records to demonstrate compliance, thus CIP-007-3, -4 Requirement R7.3 is redundant and unnecessary. This requirement has been appropriately repurposed as a measure of compliance in CIP Version 5, therefore Version 5 is consistent with, and supports, the proposed retirement of this requirement.

C. Emergency Preparedness and Operations Reliability Standards

One requirement from the EOP body of Reliability Standards is proposed for retirement**.** The EOP group of Reliability Standards consists of eight Reliability Standards that address preparation for emergencies, necessary actions during emergencies and system restoration and reporting following disturbances.[55]

1. EOP-005-2 Requirement R3.1 – System Restoration from Blackstart Resources

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

---

53 *Order on Compliance* 130 FERC ¶ 61,271 (2010).

54 *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

55 EOP-001 is dedicated to Emergency Operations Planning. EOP-002 is dedicated to Capacity and Energy Emergencies. EOP-003 is dedicated to Load Shedding Plans. EOP-004 is dedicated to Event Reporting. EOP-005 is dedicated to System Restoration Plans and Blackstart Resources. EOP-006 is dedicated to System Restoration Coordination, [note there is no EOP-007]. EOP-008 is dedicated to Loss of Control Center Functionality and EOP-009 is dedicated to Documentation of Blackstart Generating Unit Test Results.

EOP-005 is dedicated to System Restoration Plans and Blackstart Resources. The reliability purpose of EOP-005-2 is to ensure that plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure that reliability is maintained during restoration and priority is placed on restoring the Interconnection. This reliability purpose is unaffected by the proposed retirement of Requirement R3.1.

a. Procedural History

EOP-005-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[56] EOP-005-2 was submitted for Commission approval on December 31, 2009 in Docket No. RM10-16-000 and was approved on March 17, 2011 in Order No. 749.[57]

b. Technical Justification for Retirement

EOP-005-2 Requirement R3.1 requires a Transmission Operator to confirm annually that it has reviewed its restoration plan and that no changes were necessary. This requirement is redundant with EOP-005-2, Requirement R3, and therefore, the proposed retirement of this requirement is consistent with reliability principles and would create no gap in reliability.

EOP-005-2 Requirement R3 currently requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator, whether or not the plan includes changes. EOP-005-2 Requirement R3 provides:

R3. Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule.

[56] Order No. 693 at P 630.

[57] *System Restoration Reliability Standards*, 134 FERC ¶ 61,215, (March 17, 2011) ("Order No. 749"), *order on clarification*, 136 FERC ¶ 61,030 ("Order No. 749-A") (2011).

Consequently, since EOP-005-2 Requirement R3 requires the Transmission Operator to submit its restoration plan to the Reliability Coordinator whether or not there has been a change, EOP-005-2 Requirement R3.1 only adds a separate, duplicative administrative burden for the entity to also confirm that there were no changes based upon another pre-determined schedule.

For these reasons, there is no reliability gap resulting from the proposed retirement of EOP-005-2 Requirement R3.1 because a Transmission Operator already has an obligation to review and provide its restoration plan annually on a mutually agreed upon predetermined schedule to its Reliability Coordinator.

D. Facilities Design, Connections, and Maintenance Reliability Standards

Five separate Reliability Standards from the FAC body of Reliability Standards, (FAC-002; FAC-010; FAC-011; FAC-013) contain a requirement proposed for retirement, with a total of six FAC requirements proposed for retirement.

The FAC body of Reliability Standards consists of a total of nine Reliability Standards that address topics such as facility connection requirements, facility ratings, system operating limits, and transfer capabilities.[58] The FAC Reliability Standards also establish requirements for maintaining equipment and rights-of-way, including vegetation management.

1. FAC-002-1 Requirement R2 – Coordination of Plans for New Facilities

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

[58] FAC-001; FAC-002; FAC-003; FAC-008; FAC-010; FAC-011; FAC-012; FAC-013; and FAC-014.

a. Procedural History

FAC-002-0 was submitted to the Commission for approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[59] FAC-002-1 was submitted for Commission approval on September 9, 2010 in Docket No. RD10-15-000 and was approved on January 10, 2011.[60]

b. Technical Justification for Retirement

Reliability Standard FAC-002 requires that each generation owner, transmission owner, distribution provider, Load-Serving Entity ("LSE"), transmission planner and planning authority assess the impact of integrating generation, transmission and end-user facilities into the interconnected transmission system. The reliability purpose of FAC-002 is to avoid adverse impacts on reliability by requiring Generator Owners and Transmission Owners and electricity end-users to meet facility connection and performance requirements. The reliability purpose of FAC-002 is unaffected by the proposed retirement of Requirement R2.

Responsible Entities have an existing obligation to produce the same information required by Requirement R2 to demonstrate compliance with Requirement R1 and its sub-requirements, thus making Requirement R2 redundant. For this reason, the proposed retirement of Requirement R2 presents no reliability gap.

E. Interchange Scheduling and Coordination Reliability Standards

One standard from the INT body of Reliability Standards, INT-007, contains a single requirement proposed for retirement. The INT body of Reliability Standards consists of a total

[59] Order No. 693 at P 693.

[60] NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2 RD10-15-000 (January 10, 2011).

of nine Reliability Standards[61] that address interchange transactions, which occur when electricity is transmitted from a seller to a buyer across the power grid.

Reliability Standard INT-007 requires that before changing the status of submitted arranged interchanges to confirmed interchanges, the interchange authority must verify that the submitted arranged interchanges are valid and complete with relevant information and approvals from the Balancing Authorities and transmission service providers.

1. INT-007-1 Requirement R1.2 – Interchange Confirmation

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

a. Procedural History

INT-007-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[62]

b. Technical Justification for Retirement

The reliability purpose of INT-007-1 is to ensure that each Arranged Interchange is checked for reliability before it is implemented, and this purpose is unaffected by the proposed retirement of Requirement R1.2. INT-007-1 Requirement R1.2 is an administrative task that is now outdated. At one time, the identification number came from the NERC Transmission System Information Network ("TSIN") system, which is now handled via the NAESB Electric Industry Registry.[63] Also, under the E-Tag protocols, no entity may engage in an Interchange transaction without first registering with the E-Tag system and receiving an identification number. Further, the entity desiring the transaction enters this identification number in the E-

[61] INT-001; INT-003; INT-004; INT-005; INT-006; INT-007; INT-008; INT-009; and INT-010.

[62] Order No. 693 at P 867.

[63] *See, North American Energy Standards Board Webregistry Technical Guide v1.4* (Proprietary) (July 2012). The new NAESB system has updated and implemented more automation to the process.

Tag system to pre-qualify and engage in an Arranged Interchange. Accordingly, the task set forth in INT-007-1 Requirement R1.2 is an outdated activity that is no longer necessary, and thus the proposed retirement of Requirement R1.2 presents no reliability gap.

F. Interconnection Reliability Operations and Coordination

One standard from the IRO body of Reliability Standards, IRO-016, contains a single requirement proposed for retirement. The IRO body of Reliability Standards consists of twelve Reliability Standards that detail the responsibilities and authorities of a Reliability Coordinator.[64] The IRO Reliability Standards establish requirements for data, tools and wide-area view, all of which are intended to facilitate a Reliability Coordinator's ability to perform its responsibilities and ensure the reliable operation of the interconnected grid.

1. IRO-016-1 Requirement R2 – Coordination of Real-Time Activities between Reliability Coordinators

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

a. Procedural History

IRO-016-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[65]

b. Technical Justification for Retirement

IRO-016 establishes requirements for coordinated real-time operations, including: (1) notification of problems to neighboring Reliability Coordinators and (2) discussions and decisions for agreed-upon solutions for implementation. The reliability purpose of IRO-016-1 is to ensure that each Reliability Coordinator's operations are coordinated such that they will not

[64] IRO-001; IRO-002; IRO-003; IRO-004; IRO-005; IRO-006; IRO-008; IRO-009; IRO-010; IRO-014; IRO-015; and IRO-016.

[65] Order No. 693 at PP 1004-005.

have an adverse reliability impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations. To implement the purpose, IRO-016-1 Requirement R1 and its sub-requirements state:

> **R1.** The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
>
> > **R1.1.** If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.
> >
> > **R1.2.** If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
> >
> > > **R1.2.1.** If time permits, this re-evaluation shall be done before taking corrective actions.
> > >
> > > **R1.2.2.** If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

These requirements are specific actions and decision points among Reliability Coordinators that promote the reliable operation of the BES. In contrast, Requirement R2 is an administrative task and the proposed retirement will not adversely impact reliability. Therefore, the reliability purpose of IRO-016-1 is unaffected by the proposed retirement of Requirement R2.

Furthermore, outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, the retirement of IRO-016-1 Requirement R2 does not affect the ability for NERC and the Regional

Entities to require Reliability Coordinators to produce documentation to demonstrate compliance with IRO-016-1 Requirement R1 and its sub-requirements. Accordingly, retiring IRO-016-1 Requirement R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance.

G. Nuclear Reliability Standards

There is only one standard that comprises the NUC body of Reliability Standards, NUC-001, and this standard contains five requirements proposed for retirement. The NUC-001 Reliability Standard requires a nuclear plant Generator Operator to coordinate operations and planning with transmission entities providing services relating to nuclear plant operating and off-site power delivery requirements

1. NUC-001-2 Requirements R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 – Nuclear Plant Interface Coordination

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement.

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3. A requirement to review the agreement(s) at least every three years.

R9.1.4. A dispute resolution mechanism.

a. Procedural History

NUC-001-1 was submitted for Commission approval on November 19, 2007 in Docket No. RM08-3-000 and was approved on October 16, 2008.[66] NUC-001-2 was submitted for

[66] *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008) ("Order No. 716"), *order on reh'g*, Order No. 716-A, 126 FERC ¶ 61,122 (2009).

Commission approval on August 14, 2009 in Docket No. RD09-10-000 and was approved on January 21, 2010.[67]

b. Technical Justification for Retirement

The reliability purpose of NUC-001-2 is to ensure the coordination between Nuclear Plant Generator Operators and Transmission Entities for nuclear plant safe operation and shutdown. The reliability purpose of NUC-001-2 is unaffected by the proposed retirement of Requirements 9.1, 9.1.1, 9.1.2, 9.1.3 and 9.1.4. Requirement 9.1 and its sub-requirements specify certain administrative elements that must be included in the agreement (required by R2) between the Nuclear Plant Generator Operator and the applicable Transmission Entities. These are a mix of technical, communication, training and administrative requirements. Requirement R9.1 and its sub-requirements are administrative tasks and the proposed retirement of these Requirements will not adversely impact reliability. Further, requiring via a mandatory Reliability Standard the inclusion of boilerplate provisions is unnecessarily burdensome relative to the other significant requirements in NUC-001-2 that pertain to performance based reliability coordination and protocols between Transmission Entities and Nuclear Plant Generator Operators. Therefore, the proposed retirement of NUC-001-2 R9.1 and all its sub-requirements creates no reliability gap.

H. Protection and Control Reliability Standards

Two standards from the PRC body of Reliability Standards, PRC-010 and PRC-022, contain a requirement proposed for retirement. PRC systems on Bulk-Power System elements are an integral part of reliable grid operation. Protection systems are designed to detect and isolate faulty elements on a system, thereby limiting the severity and spread of system disturbances, and preventing possible damage to protected elements. The function, settings, and

[67] *Order Approving Reliability Standard*, 130 FERC ¶ 61,051 (2010).

limitations of a protection system are critical in establishing System Operating Limits and Interconnection Reliability Operating Limits. The PRC Reliability Standards consist of a total of twenty-three Reliability Standards that apply to Transmission Operators, Transmission Owners, Generator Operators, Generator Owners, Distribution Providers and Regional Reliability Organizations and cover a wide range of topics related to the protection and control of power systems.[68]

1. PRC-010-0 Requirement R2 – Assessment of the Design and Effectiveness of UVLS Program

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

a. Procedural History

PRC-010-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[69]

b. Technical Justification for Retirement

Reliability Standard PRC-010 requires transmission owners, transmission operators, LSEs and distribution providers to periodically conduct and document an assessment of the effectiveness of their Under Voltage Load Shedding ("UVLS") program at least every five years or as required by changes in system conditions. The assessment must be conducted with the associated transmission planner and planning authority. The purpose of PRC-010 is to provide system preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an UVLS program. Outside the context of a Reliability Standard,

[68] PRC-001; PRC-002; PRC-003; PRC-004; PRC-005; PRC-006; PRC-007, PRC-008; PRC-009; PRC-010; PRC-011; PRC-012; PRC-013; PRC-014; PRC-015; PRC-016; PRC-017; PRC-018; PRC-019; PRC-020; PRC-021; PRC-022; and PRC-023.

[69] Order No. 693 at P 1509.

under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its current UVLS program assessment for purposes of monitoring compliance. Thus, the retirement of PRC-010-0 Requirement R2 does not affect the ability of NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-010-0 Requirement R1 and its sub-requirements. Furthermore, PRC-010-0 Requirement R1 requires that the entity document an assessment of the effectiveness of its UVLS program:

> The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program.

Accordingly, the proposed retirement of PRC-010-0 Requirement R2 presents no reliability gap.

2. PRC-022-1 Requirement R2 – Under-Voltage Load Shedding Program Performance

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

a. Procedural History

PRC-022-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[70]

b. Technical Justification for Retirement

The purpose of Reliability Standard PRC-022 is to ensure that UVLS programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the BES. PRC-022 requires transmission operators, LSEs, and distribution providers to provide analysis,

[70] Order No. 693 at P 1565.

documentation, and misoperation data on UVLS operations to the regional reliability organization.

PRC-022-1, Requirement R2 requires entities to provide documentation of its analysis of its UVLS program performance within 90 days of request. The proposed retirement of PRC-022-1, Requirement R2 is consistent with reliability principles and will not result in a gap in reliability as NERC has the ability to request this information pursuant to Section 400 of the NERC Rules of Procedure. Thus, the proposed retirement of PRC-022-1 Requirement R2 does not affect the ability of NERC to require Reliability Coordinators to produce documentation to monitor compliance with PRC-022-1 Requirement R1 and its sub-requirements. Furthermore, PRC-022-1 Requirement R1 also requires that the entity document its UVLS performance:

> Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations.

Accordingly, the proposed retirement of PRC-022-1 Requirement R2 presents no gap to reliability. The ERO compliance program efficiency will increase since it will no longer need to track a static requirement of whether a UVLS program assessment was submitted within 30 days of a request by NERC or the Regional Entity, and instead, compliance monitoring may focus on the more substantive requirements of PRC-022-1.

I. Voltage and Reactive Reliability Standards

One standard from the VAR body of Reliability Standards, VAR-001, contains a single requirement proposed for retirement. VAR-001 is dedicated to Voltage and Reactive Control and VAR-002 is dedicated to Generator Operation for Maintaining Network Voltage Schedules. VAR-001 ensures that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real-time to protect equipment and the reliable

operation of the Interconnection. VAR-002 ensures that generators provide reactive and voltage control necessary to ensure voltage levels, reactive flows, and reactive resources are maintained within applicable Facility Ratings to protect equipment and the reliable operation of the Interconnection. These two Reliability Standards, along with two regional standards (VAR-002-WECC-1 and VAR-501-WECC-1), form the VAR Reliability Standards.

1. VAR-001-2, Requirement R5 – Voltage and Reactive Control

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

a. Procedural History

VAR-001-1 was submitted for Commission approval on April 4, 2006, in Docket No. RM06-16-000 and approved by the Commission in Order No. 693.[71] When approving VAR-001-1, in Order No. 693 at paragraph 1858, the Commission recognized:

> [T]hat all transmission customers of public utilities are required to purchase Ancillary Service No. 2 under the OATT or self-supply, but the OATT does not require them to provide information to transmission operators needed to accurately study reactive power needs. The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities.

On September 9, 2010, NERC submitted VAR-001-2, which included revisions to Requirement R5 to satisfy Commission directives in Order No. 693, including the directive in paragraph 1858. This directive was addressed by adding "Load Serving Entities" to the standard as applicable entities and making them subject to the same requirements as purchasing-selling entities

[71] Order No. 693 at P 1880.

("PSEs"). These modifications to VAR-001-2 were accepted by the Commission on January 10, 2011.[72]

b. Technical Justification for Retirement

The proposed retirement of VAR-001-2, Requirement R5 is consistent with reliability principles as this Requirement is (i) redundant with the Commission's *pro forma* open access transmission tariff ("OATT"); and (ii) the reliability objective is achieved via VAR-001-2, Requirement R2.

VAR-001-2, Requirement R5 provides for the PSE and LSE (transmission customers) to arrange for or self-provide reactive resources as required under Schedule 2 of the OATT. Schedule 2 of the OATT states:

> **Schedule 2 Reactive Supply and Voltage Control from Generation or Other**
> In order to maintain transmission voltages on the Transmission Provider's transmission facilities within acceptable limits, generation facilities and non-generation resources capable of providing this service that are under the control of the control area operator) are operated to produce (or absorb) reactive power. Thus, Reactive Supply and Voltage Control from Generation or Other Sources Service must be provided for each transaction on the Transmission Provider's transmission facilities. The amount of Reactive Supply and Voltage Control from Generation or Other Sources Service that must be supplied with respect to the Transmission Customer's transaction will be determined based on the reactive power support necessary to maintain transmission voltages within limits that are generally accepted in the region and consistently adhered to by the Transmission Provider.
>
> Reactive Supply and Voltage Control from Generation or Other Sources Service is to be provided directly by the Transmission Provider (if the Transmission Provider is the Control Area operator) or indirectly by the Transmission Provider making arrangements with the Control Area operator that performs this service for the Transmission Provider's Transmission System. The Transmission Customer must purchase this service from the Transmission Provider or the Control Area operator. A Transmission Customer may satisfy all or part of its obligation through self provision or purchases provided that the self-provided or purchased reactive power reduces the Transmission Provider's reactive power requirements and is from generating facilities under the control of the

[72] *North American Electric Reliability Corp.*, 134 FERC ¶ 61,015 (2011).

> Transmission Provider or Control Area operator. The Transmission Customer's Service Agreement shall specify any such reactive supply arrangements. To the extent the Control Area operator performs this service for the Transmission Provider, charges to the Transmission Customer are to reflect only a pass-through of the costs charged to the Transmission Provider by the Control Area operator. The Transmission Provider's rates for Reactive Supply and Voltage Control from Generation Sources Services shall be set out in Appendix A to this Schedule.

Given the importance of the procurement or self-provision of reactive power, even in a market setting, a form of Schedule 2 is found in the tariffs of MISO and PJM, for example. Also, other contractual mechanisms, such as Interchange agreements, also are used to ensure transmission customers (such as PSEs and LSEs) provide reactive power. While NERC complied with the Commission's directive to add LSEs to VAR-001-2 Requirement R5, a review of this requirement in light of Schedule 2 indicates that the reliability objective of ensuring that PSEs as well as LSEs either acquire or self provide reactive power resources associated with transmission service requests is accomplished via Schedule 2, and, therefore, there is no need to reiterate it in VAR-001-2 Requirement R5. The repetitive nature of VAR-001-2 Requirement R5 is also apparent in the context of how a PSE or LSE generally demonstrates compliance – via screenshots from Open Access Same-Time Information System reservations that show the mandatory acquiring or self providing of reactive power resources per Schedule 2.

The reliability objective of VAR-001-2 is also accomplished in VAR-001-2 Requirement R2 (that is not proposed for retirement) which reads:

> Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, [sic] and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

The Transmission Operator's adherence to Requirement R2 is a double-check for the obligations under Schedule 2 to ensure there are sufficient reactive power resources to protect the voltage

levels under normal and Contingency conditions. This double check, however, does not relieve PSEs and LSEs from their obligations under Schedule 2 of the OATT or Interchange agreements.

In addition, in the Electric Reliability Council of Texas ("ERCOT") region, where there is no FERC approved OATT, reactive power is handled via Section 3.15 of the ERCOT Nodal Protocols that describes how ERCOT establishes a voltage profile for the grid, and then in detail explains the responsibilities of the Generators, Distribution Providers and Texas Transmission Service Providers (not to be confused with a NERC Transmission Service Provider), to meet the Voltage Profile and ensure that those entities have sufficient reactive support to do so. There is further Operating Guide detail on the responsibilities for entities to deploy reactive resources approximately, within performance criteria in the Operating Guide Section 3. Thus, as in non-ERCOT regions, ERCOT has protocols that are duplicative of VAR-001-2, Requirement R5. Given the redundant nature of VAR-001-2 Requirement R5, the proposed retirement of this requirement presents no reliability gap.

V. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission:

- approve the proposed retirement of Reliability Standard Requirements and associated elements included in **Exhibit B,** effective as proposed herein; and

- approve the implementation plan included in **Exhibit C**;

Respectfully submitted,

/s/ Stacey Tyrewala

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

Counsel for the North American Electric Reliability Corporation

Dated: February 28, 2013

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 28th day of February, 2013.

/s/ Stacey Tyrewala

Stacey Tyrewala

Attorney for North American Electric Reliability Corporation

Exhibit A

Paragraph 81 Criteria

Exhibit A — Paragraph 81 Criteria

Paragraph 81 Criteria

The P 81 Team developed three criteria: (1) Criteria A: an overarching criteria designed to determine that there is no reliability gap created by the proposed retirement; (2) Criteria B: which consists of seven separate identifying criteria designed to recognize requirements appropriate for retirement; and (3) Criteria C: which consists of seven separate questions designed to assist the P 81 Team in making an informed decision regarding whether requirements are appropriate to propose for retirement.

In order for a Reliability Standard Requirement to be proposed for retirement, it must satisfy *both*: (i) Criteria A (the overarching criterion) and (ii) at least one of the Criteria B (identifying criteria). In addition, the data and reference points set forth below in Criteria C were considered to make a more informed decision on whether to proceed with retirement.

Criterion A (Overarching Criterion)
The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

This criterion is based on the Commission's language in P 81 of the March 15th Order.

Section 215(a)(4) of the Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

Criteria B (Identifying Criteria)

B1. ***Administrative***
The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

This criterion is designed to identify Requirements that can be removed with little effect on reliability and whose removal will result in an increase in the efficiency of the ERO compliance program. Administrative functions may include a task that is or is not related to

developing procedures or plans, such as establishing communication contacts. Thus, for certain requirements, Criterion B1 is closely related to Criteria B2, B3 and B4. Strictly administrative functions do not inherently impact reliability directly and, where possible, should be eliminated for purposes of efficiency and to allow the ERO and entities to allocate resources appropriately.

B2. ***Data Collection/Data Retention***
These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

This criterion is designed to identify requirements that can be removed with little effect on reliability. The collection and/or retention of data do not necessarily have a reliability benefit and yet are often required to demonstrate compliance. Where data collection and/or data retention is unnecessary for reliability purposes, such requirements should be eliminated in order to increase the efficiency of the ERO compliance program.

B3. ***Documentation***
The Reliability Standard requirement requires responsible entities to develop a document (e.g., plan, policy or procedure) which is not necessary to protect BES reliability.

This criterion is designed to identify requirements that require the development of a document that is unrelated to reliability or has no performance or results-based function. In other words, the document is required, but no execution of a reliability activity or task is associated with or required by the document.

B4. ***Reporting***
The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity.

This criterion is designed to identify requirements that obligate Responsible Entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement, there would be little impact on reliability.

B5. ***Periodic Updates***
The Reliability Standard requirement requires responsible entities to periodically update (e.g., annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

This criterion is designed to identify requirements that impose an updating requirement that is out of sync with the actual operations of the BES, unnecessary or duplicative.

B6. ***Commercial or Business Practice***
The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

This criterion is designed to identify those requirements that require: (i) implementing a best or outdated business practice or (ii) implicating the exchange of or debate on commercially sensitive information while doing little, if anything, to promote the reliable operation of the BES.

B7. ***Redundant***
The Reliability Standard requirement is redundant with: (i) another FERC-approved Reliability Standard requirement(s); (ii) the ERO compliance and monitoring program or (iii) a governmental regulation (e.g., Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

This criterion is designed to identify requirements that are redundant with other requirements and are, therefore, unnecessary. Unlike the other criteria listed in Criterion B, in the case of redundancy, the task or activity itself may contribute to a reliable BES, but it is not necessary to have two duplicative requirements on the same or similar task or activity. Such requirements can be removed with little or no effect on reliability and removal will result in an increase in efficiency of the ERO compliance program.

Criteria C (Additional Data and Reference Points)

To assist in the determination of whether to proceed with the retirement of a Reliability Standard requirement that satisfied both Criteria A and B, the following data and reference points were considered by the P 81 Team to make a more informed decision:

C1. Was the Reliability Standard requirement part of a FFT filing?

This criterion was applied in order to determine what efficiencies would be gained for the NERC compliance program.

C2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?

This criterion was applied in order to determine whether the requirement proposed for retirement was a part of an active on-going standard development project.

C3. What is the VRF of the Reliability Standard requirement?

Each requirement must have an associated violation risk factor ("VRF") (High, Medium, or Lower). The risk factor is one of several elements used to determine an appropriate sanction when the associated requirement is violated. The risk factor assesses the impact to reliability of violating a specific requirement. This criterion was applied in order to determine what efficiencies would be gained for the NERC compliance program.

C4. In which tier of the 2013 AML does the Reliability Standard requirement fall?

The NERC Actively Monitored List ("AML") is the minimum scope of compliance audits and consists of a three tiered approach.

- Tier 1 Requirements are those that are the most critical to the purpose and intent of the standard of which they are a part. Additionally, the ability of a registered entity to demonstrate compliance with Tier 1 Requirements will provide guidance to audit teams on the necessity to investigate further and broaden an audit's scope in additional Requirements or reliability standards or both.

- Tier 2 Requirements are also critical to the purpose of a standard, but less so than Tier 1 in that Tier 2 does not address the ERO high-risk priorities as directly as Tier 1. Tier 2 also does not pose as severe a risk as Tier 1. The determination of

what tier each assignment is assigned is done using all the data and input mentioned earlier in this section of the report, applied with professional judgment and input from the Regional Entities. This is not to say that compliance with Tier 2 Requirements is not mandatory. Instead, Tier 2 Requirements represent an additional level of inquiry that must be undertaken when a registered entity does not display clear compliance with those most critical Requirements of Tier 1. In the process of this added level of investigation, it may become necessary to branch off into other reliability standards that were not identified as relating directly to an ERO priority.

- Tier 3 Requirements are those that, while still being significant to Bulk-Power System reliability, do not represent the purpose of a reliability standard directly or are not representative of ERO priorities. The exploration of an audit team into the compliance of a registered entity with Tier 3 Requirements will be initiated through links between identified deficiencies in Tier 1 and 2 Requirements and those of Tier 3.

Note, Registered Entities are responsible for compliance with all regulatory approved reliability standards and requirements in effect per their registered functions at all times, regardless of what is specified in the AML.

C5. Is there a possible negative impact on NERC's published and posted reliability principles?

The application of this criterion involves consideration of eight reliability principles published on the NERC webpage.[73]

C6. Is there any negative impact on the defense in depth protection of the Bulk Electric System?

This criterion is designed to assess whether other Requirements rely on the Requirement proposed for retirement to protect the BES, in recognition of the fact that NERC Reliability Standards are an integrated whole.

C7. Does the retirement promote results or performance based Reliability Standards?

Generally, NERC strives to achieve results-based Reliability Standards, which contain results-based requirements with sufficient clarity to hold entities accountable without being overly prescriptive as to how a specific reliability outcome is to be achieved. This criterion is designed to ensure that the P 81 Project is consistent with this direction.

[73] Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.
Principle 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.
Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
Principle 7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.
Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks. (footnote omitted).

Exhibit B

Redlined Version of Reliability Standards with Proposed Retirements

A. Introduction

1. **Title:** **Automatic Generation Control**

2. **Number:** BAL-005-0.2b

3. **Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.

4. **Applicability:**

   4.1. Balancing Authorities

   4.2. Generator Operators

   4.3. Transmission Operators

   4.4. Load Serving Entities

5. **Effective Date:** May 13, 2009

B. Requirements

R1. All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.

R1.1. Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.

R1.2. Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.

R1.3. Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retired)

R3. A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.

R4. A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.

R5. A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.

R6. The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

R7. The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.

R8. The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.

R8.1. Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.

R9. The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.

R9.1. Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.

R10. The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.

R11. Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.

R12. Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.

R12.1. Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.

R12.2. Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.

R12.3. Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.

R13. Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.

R14. The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.

R15. The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

R16. The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

1.1.1. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.

1.1.2. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

1.3.1. Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.

1.3.2. Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Effective Date: August 27, 2008 (U.S.)

Interpretation of BAL-005-0 Automatic Generation Control, R17

Request for Clarification received from PGE on July 31, 2007

PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

BAL-005-0

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25% of full scale
Remote terminal unit	≤ 0.25% of full scale
Potential transformer	≤ 0.30% of full scale
Current transformer	≤ 0.50% of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to "annually check and calibrate" does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to "annually check and calibrate" the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system

operator. Frequency inputs from other sources that are for reference only are excluded. The time error and frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-3

3. Purpose: Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-003-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-3 Requirement R2.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

	3	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within thirty calendar days of the effective date.	
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3. (Retired)	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1. (Retired)	LOWER	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
R3.2. (Retired)	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3. (Retired)	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	The Responsible Entity has established but not documented a change	The Responsible Entity has established but not documented both a change control process and configuration management	The Responsible Entity has not established and documented a change control process OR	The Responsible Entity has not established and documented a change control process AND

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		control process OR The Responsible Entity has established but not documented a configuration management process.	process.	The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a configuration management process.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-3a

3. Purpose: Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability

4.1. Within the text of Standard CIP-005-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-3, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-3 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity	

		shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation
3a	02/02/11	Approved by FERC	
3a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal

Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	and Standard CIP-009-4.	and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter.		
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6. (Retired)	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.			
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to designated response personnel.	Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	Revised.
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"
4a	4/19/12	FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3a, 4a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

3. Purpose: Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-007-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-3 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical)	

		Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
3	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, **but did not document** that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).

		testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).		
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.
R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program **but** did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.

R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.

R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
R5.1.1.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

			manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).		
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 **but** did not maintain records as specified in R7.3. (Retired)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A
R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3. (Retired)	LOWER	N/A	N/A	N/A	N/A

Formatted: Font color: Red

R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A
R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

E. **Regional Variances**

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Restoration from Blackstart Resources**

2. Number: EOP-005-2

3. Purpose: Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

4. Applicability:

4.1. Transmission Operators.

4.2. Generator Operators.

4.3. Transmission Owners identified in the Transmission Operators restoration plan.

4.4. Distribution Providers identified in the Transmission Operators restoration plan.

5. Proposed Effective Date: Twenty-four months after the first day of the first calendar quarter following applicable regulatory approval. In those jurisdictions where no regulatory approval is required, all requirements go into effect twenty-four months after Board of Trustees adoption.

B. Requirements

R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Time Horizon = Operations Planning]*

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

R1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

R1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.

R2. Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. *[Time Horizon = Operations Planning]*

R3. Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule. *[Time Horizon = Operations Planning]*

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary. (Retired)

R4. Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan. *[Time Horizon = Operations Planning]*

R4.1. Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.

R5. Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date. *[Time Horizon = Operations Planning]*

R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify: *[Time Horizon = Long-term Planning]*

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

R7. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each

affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration. *[Time Horizon = Real-time Operations]*

R8. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator. *[Time Horizon = Real-time Operations]*

R9. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Time Horizon = Operations Planning]*

R9.1. The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

R9.2. A list of required tests including:

R9.2.1. The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.

R9.2.2. The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

R9.3. The minimum duration of each of the required tests.

R10. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following: *[Time Horizon = Operations Planning]*

R10.1. System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.

R10.2. Restoration priorities.

R10.3. Building of cranking paths.

R10.4. Synchronizing (re-energized sections of the System).

R11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks. *[Time Horizon = Operations Planning]*

R12. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Time Horizon = Operations Planning]*

R13. Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. *[Time Horizon = Operations Planning]*

R14. Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. *[Time Horizon = Operations Planning]*

R15. Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator's restoration plan within 24 hours following such change. *[Time Horizon = Operations Planning]*

R16. Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. *[Time Horizon = Operations Planning]*

R16.1. Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R9.

R16.2. Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.

R17. Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: *[Time Horizon = Operations Planning]*

R17.1. System restoration plan including coordination with the Transmission Operator.

R17.2. The procedures documented in Requirement R14.

R18. Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator. *[Time Horizon = Operations Planning]*

C. Measures

M1. Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator.

M2. Each Transmission Operator shall have evidence such as e-mails with receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan in accordance with Requirement R2.

M3. Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, e-mails with receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.

M4. Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, e-mails with receipts, or registered mail receipts, that it has updated its restoration plan and submitted it to its Reliability Coordinator in accordance with Requirement R4.

M5. Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan available in its primary and backup control rooms and its System Operators prior to its implementation date in accordance with Requirement R5.

M6. Each Transmission Operator shall have documentation such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.

M7. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved shall have evidence such as voice recordings, e-mail, dated computer printouts, or operator logs, that it implemented its restoration plan or restoration plan strategies in accordance with Requirement R7.

M8. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved in such an event shall have evidence, such as voice recordings, e-mail, dated computer printouts, or operator logs, that it resynchronized shut down areas in accordance with Requirement R8.

M9. Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R9.

M10. Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R10.

M11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R11.

M12. Each Transmission Operator shall have evidence, such as training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R12.

M13. Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R13.

M14. Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R14.

M15. Each Generator Operator with a Blackstart Resource shall provide evidence, such as e-mails with receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within twenty-four hours of such changes in accordance with Requirement R15.

M16. Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R16.

M17. Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R17.

M18. Each Generator Operator shall have evidence, such as dated training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R18.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Approved restoration plan and any restoration plans in force since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of an updated restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three years for Requirement R4, Measure M4.
- The current, restoration plan approved by the Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- Implementation of its restoration plan or restoration plan strategies on any occasion for three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R7, Measure M7.
- Resynchronization of shut down areas on any occasion over three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R8, Measure M8.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R9, Measure M9.
- Actual training program materials or descriptions for three calendar years for Requirement R10, Measure M10.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit as well as one previous compliance audit period for Requirement R12, Measure M12.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator, applicable Transmission Owner, and applicable Distribution provider shall keep data or evidence to show compliance as identified

below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Actual training program materials or descriptions and actual training records for three calendar years for Requirement R11, Measure M11.

If a Transmission Operator, applicable Transmission owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in force since its last compliance audit for Requirement R13, Measure M13.

The Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current documentation and any documentation in force since its last compliance audit on procedures to start each Blackstart Resources and for energizing a bus for Requirement R14, Measure M14.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R15, Measure M15.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R16, Measure M16.
- Actual training program materials and actual training records for three calendar years for Requirement R17, Measure M17.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Generator Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R18, Measure M18.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	May 2, 2007	Approved by Board of Trustees	Revised
2	TBD	Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-005-2 (approval effective 5/23/11)	
2	TBD	R3.1 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Coordination of Plans For New Generation, Transmission, and End-User Facilities

2. Number: FAC-002-1

3. Purpose: To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.

4. Applicability:

4.1. Generator Owner

4.2. Transmission Owner

4.3. Distribution Provider

4.4. Load-Serving Entity

4.5. Transmission Planner

4.6. Planning Authority

5. (Proposed) Effective Date: The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:

1.1. Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.

1.2. Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.

1.3. Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.

1.4. Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.

1.5. Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected

transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days). (Retired)

C. Measures

M1. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider's documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.

M2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Timeframe

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting

Complaints

1.4. Data Retention

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

1.5. Additional Compliance Information

None

2. Violation Severity Levels (no changes)

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata
1	TBD	Modified to address Order No. 693 Directives contained in paragraph 693.	Revised.

1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Facility Ratings**

2. **Number:** FAC-008-3

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.

4. **Applicability**

   4.1. Transmission Owner.

   4.2. Generator Owner.

5. **Effective Date:** The first day of the first calendar quarter that is twelve months beyond the date approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter twelve months following BOT adoption.

B. Requirements

R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:

- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
- Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:

2.2.1. Equipment Rating standard(s) used in development of this methodology.

2.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

2.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

2.2.4. Operating limitations.[1]

2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.4. The process by which the Rating of equipment that comprises a Facility is determined.

2.4.1. The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

2.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R3. Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

3.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:

3.2.1. Equipment Rating standard(s) used in development of this methodology.

[1] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

3.2.4. Operating limitations.[2]

3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

3.4. The process by which the Rating of equipment that comprises a Facility is determined.

3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R7. Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

[2] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

8.1. As scheduled by the requesting entities:

8.1.1. Facility Ratings

8.1.2. Identity of the most limiting equipment of the Facilities

8.2. Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1. Identity of the existing next most limiting equipment of the Facility

8.2.2. The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

C. Measures

M1. Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.

M2. Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.

M3. Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.

M4. Each Transmission Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement 4. The Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its documentation for determining its Facility Ratings or its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement R4. (Retired)

M5. If the Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology or a Generator Owner's documentation for determining its Facility Ratings, the Transmission Owner or Generator Owner shall have evidence, (such as a copy of a dated electronic or hard copy note, or other comparable evidence from the Transmission Owner or Generator Owner addressed to the commenter that includes the response to the comment,) that it provided a response to that commenting entity in accordance with Requirement R5. (Retired)

M6. Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).

M7. Each Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R7.

M8. Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability

Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority**

Regional Entity

1.2. **Compliance Monitoring and Enforcement Processes:**

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting
- Compliance Violation Investigations
- Complaints

1.3. **Data Retention**

The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.

The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.

The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.

The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.

The Generator Owner and Transmission Owner shall each keep evidence for Measure M4, and Measure M5, for three calendar years. (Retired)

The Generator Owner shall keep evidence for Measure M7 for three calendar years.

The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.

If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. **Additional Compliance Information**

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	• The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part 2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
R3	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	• 3.2.2 • 3.2.3 • 3.2.4	• 3.2.2 • 3.2.3 • 3.2.4	OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
R4 (Retired)	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.	The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.	The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)
R5 (Retired)	The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)	The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)	The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation. (R5)	The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
R7	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the requesting entities.
R8	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1)	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)	than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)

Formatted Table

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	
3	TBD	R4 and R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

A. Introduction

1. Title: **System Operating Limits Methodology for the Planning Horizon**

2. Number: FAC-010-2.1

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable planning of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Planning Authority

5. Effective Date: April 19, 2010

B. Requirements

R1. The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the planning horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R2.5. Starting with all Facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.6. In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:

R2.6.1. Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers.

R3. The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).

R3.2. Selection of applicable Contingencies.

R3.3. Level of detail of system models used to determine SOLs.

R3.4. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.5. Anticipated transmission system configuration, generation dispatch and Load level.

R3.6. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.

R4. The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:

R4.1. Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.

R4.2. Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.

R4.3. Each Transmission Planner that works in the Planning Authority's Planning Authority Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. Measures

M1. The Planning Authority's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Planning Authority shall have evidence it issued its SOL Methodology and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Planning Authority that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Planning Authority shall self-certify its compliance to the Compliance Monitor at least once every three years. New Planning Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Planning Authority shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

Formatted: Strikethrough

Formatted: Font color: Red

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Planning Authority shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology. (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R2.1 through R2.3 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.2	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
R2	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 –R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
R3	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
R4	One or both of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority failed to issue its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but

Requirement	Lower	Moderate	High	Severe
				four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
R5 (Retired)	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

E. **Regional Differences**

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-010.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
1	November 1, 2006	Fixed typo. Removed the word "each" from the 1st sentence of section D.1.3, Data Retention.	01/11/07
2	June 24, 2008	Adopted by Board of Trustees; FERC Order 705	Revised
2		Changed the effective date to July 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2.1	November 5, 2009	Adopted by the Board of Trustees — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	April 19, 2010	FERC Approved — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Operating Limits Methodology for the Operations Horizon**

2. Number: FAC-011-2

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: April 29, 2009

B. Requirements

R1. The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the operations horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. In determining the system's response to a single Contingency, the following shall be acceptable:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in FAC-011 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. Interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies

R2.3.3. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R3. The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)

R3.2. Selection of applicable Contingencies

R3.3. A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.

R3.3.1. This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies.

R3.4. Level of detail of system models used to determine SOLs.

R3.5. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.6. Anticipated transmission system configuration, generation dispatch and Load level

R3.7. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_V.

R4. The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:

R4.1. Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.

R4.2. Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.

R4.3. Each Transmission Operator that operates in the Reliability Coordinator Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. **Measures**

M1. The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Reliability Coordinator that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5 (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

Formatted: Strikethrough

Formatted: Font color: Red

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R3.1, R3.2, R3.4 through R3.7 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.1, R3.2, R3.4 through R3.7.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4.

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
R4	One or both of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to

Requirement	Lower	Moderate	High	Severe
				30 calendar days after the effectiveness of the change.
R5 (Retired)	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

2. Number: FAC-013-2

3. Purpose: To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.

4. Applicability:

4.1. Planning Coordinators

5. Effective Date:

In those jurisdictions where regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after applicable regulatory approval or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-2 are effective.

In those jurisdictions where no regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after Board of Trustees adoption or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1 and MOD-030-2 are effective.

B. Requirements

R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Criteria for the selection of the transfers to be assessed.

1.2. A statement that the assessment shall respect known System Operating Limits (SOLs).

1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's planning practices.

1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:

1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.

1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.

1.4.3. System demand.

1.4.4. Current approved and projected Transmission uses.

1.4.5. Parallel path (loop flow) adjustments.

1.4.6. Contingencies

1.4.7. Monitored Facilities.

1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.

R2. Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. Distribute to the following prior to the effectiveness of such revisions:

2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.

2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.

2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]* (Retired)

R4. During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

R5. Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

R6. If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

C. Measures

M1. Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.

M2. Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2

M3. Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. (Retired)

M4. Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.

M5. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5.

M6. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Data Retention

The Planning Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. (R3 retired)
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.

Formatted Table

Formatted Table

R2	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.
R3 **(Retired)**	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.

R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.

Formatted Table

R5	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.

Formatted Table

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	08/01/05	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Lower cased the word "draft" and "drafting team" where appropriate. 3. Changed Anticipated Action #5, page 1, from "30-day" to "Thirty-day." 4. Added or removed "periods."	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	5/17/12	FERC Order issued directing the VRF's for Requirements R1. and R4. be changed from "Lower" to "Medium." FERC Order issued correcting the High and Severe VSL language for R1.	
2	TBD	R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Interchange Confirmation**

2. Number: **INT-007-1**

3. Purpose: To ensure that each Arranged Interchange is checked for reliability before it is implemented.

4. Applicability

4.1. Interchange Authority.

5. Effective Date: January 1, 2007

B. Requirements

R1. The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:

R1.1. Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry. (Retired)

R1.3. The following are defined:

R1.3.1. Generation source and load sink.

R1.3.2. Megawatt profile.

R1.3.3. Ramp start and stop times.

R1.3.4. Interchange duration.

R1.4. Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.

C. Measures

M1. For each Arranged Interchange, the Interchange Authority shall show evidence that it has verified the Arranged Interchange information prior to the dissemination of the Confirmed Interchange.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Time Frame

The Performance-Reset Period shall be twelve months from the last noncompliance to Requirement 1.

1.3. Data Retention

The Interchange Authority shall keep 90 days of historical data. The Compliance Monitor shall keep audit records for a minimum of three calendar years.

1.4. Additional Compliance Information

Each Interchange Authority shall demonstrate compliance to the Compliance Monitor within the first year that this standard becomes effective or the first year the entity commences operation by self-certification to the Compliance Monitor.

Subsequent to the initial compliance review, compliance may be:

1.4.1 Verified by audit at least once every three years.

1.4.2 Verified by spot checks in years between audits.

1.4.3 Verified by annual audits of noncompliant Interchange Authorities, until compliance is demonstrated.

1.4.4 Verified at any time as the result of a complaint. Complaints must be lodged within 60 days of the incident. Complaints will be evaluated by the Compliance Monitor.

Each Interchange Authority shall make the following available for inspection by the Compliance Monitor upon request:

1.4.5 For compliance audits and spot checks, relevant data and system log records for the audit period which indicate an Interchange Authority's verification that all Arranged Interchange was balanced and valid as defined in R1. The Compliance Monitor may request up to a three-month period of historical data ending with the date the request is received by the Interchange Authority.

1.4.6 For specific complaints, only those data and system log records associated with the specific Interchange event contained in the complaint which indicate an Interchange Authority's verification that an Arranged Interchange was balanced and valid as defined in R1 for that specific Interchange

2. Levels of Non-Compliance

2.1. Level 1: One occurrence[1] where Interchange-related data was not verified as defined in R1.

2.2. Level 2: Two occurrences where Interchange-related data was not verified as defined in R1.

2.3. Level 3: Three occurrences where Interchange-related data was not verified as defined in R1.

2.4. Level 4: Four or more occurrences where Interchange-related data was not verified as defined in R1.

E. Regional Differences

None

[1] This does not include instances of not verifying due to extenuating circumstances approved by the Compliance Monitor.

Version History

Version	Date	Action	Change Tracking
1	TBD	R1.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Coordination of Real-time Activities Between Reliability Coordinators**

2. Number: **IRO-016-1**

3. Purpose: To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: November 1, 2006

B. Requirements

R1. The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.

R1.1. If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.

R1.2. If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).

R1.2.1. If time permits, this re-evaluation shall be done before taking corrective actions.

R1.2.2. If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

R1.3. If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both. (Retired)

C. Measures

M1. For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

The performance reset period shall be one calendar year.

1.3. Data Retention

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

1.4. Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction's discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

2. Levels of Non-Compliance

2.1. Level 1: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
Version 1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Hyphenated "30-day" and "Reliability Coordinator-to-Reliability Coordinator" when used as adjective.	01/20/06

		3. Changed standard header to be consistent with standard "Title." 4. Added "periods" to items where appropriate. 5. Initial capped heading "Definitions of Terms Used in Standard." 6. Changed "Timeframe" to "Time Frame" in item D, 1.2. 7. Lower cased all words that are not "defined" terms — drafting team, and self-certification. 8. Changed apostrophes to "smart" symbols. 9. Removed comma after word "condition" in item R.1.1. 10. Added comma after word "expected" in item 1.4, last sentence. 11. Removed extra spaces between words where appropriate.	
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Nuclear Plant Interface Coordination**

2. Number: NUC-001-2

3. Purpose: This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. Applicability:

4.1. Nuclear Plant Generator Operator.

4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

4.2.1 Transmission Operators.

4.2.2 Transmission Owners.

4.2.3 Transmission Planners.

4.2.4 Transmission Service Providers.

4.2.5 Balancing Authorities.

4.2.6 Reliability Coordinators.

4.2.7 Planning Coordinators.

4.2.8 Distribution Providers.

4.2.9 Load-serving Entities.

4.2.10 Generator Owners.

4.2.11 Generator Operators.

5. Effective Date: April 1, 2010

B. Requirements

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Medium*]

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

R4.1. Incorporate the NPIRs into their operating analyses of the electric system.

R4.2. Operate the electric system to meet the NPIRs.

R4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

R5. The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]

R9.1. Administrative elements: (Retired)

R9.1.1. Definitions of key terms used in the agreement. (Retired)

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. (Retired)

R9.1.3. A requirement to review the agreement(s) at least every three years. (Retired)

R9.1.4. A dispute resolution mechanism. (Retired)

R9.2. Technical requirements and analysis:

R9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

R9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

R9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

R9.3. Operations and maintenance coordination:

R9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

R9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

R9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

R9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

R9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. .

R9.3.6. Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

R9.3.7. Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

R9.4. Communications and training:

R9.4.1. Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

R9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

R9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

R9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

R9.4.5. Provisions for personnel training, as related to NPIRs.

C. Measures

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. (Requirement 2 and 9)

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:

M4.1 The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)

M4.2 The electric system was operated to meet the NPIRs. (Requirement 4.2)

M4.3 The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)

M8. The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

2.1. Lower: Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.

2.2. Moderate: Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.

2.3. High: One or more requirements of R3 through R8 were not met.

2.4. Severe: No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

E. Regional Differences

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs.
Therefore the definition of NPLR for Canadian CANDU units will be as follows:

Nuclear Plant Licensing Requirements (NPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	Revision
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update
2	TBD	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.**

2. Number: PRC-010-0

3. Purpose: Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.

4. Applicability:

4.1. Load-Serving Entity that operates a UVLS program

4.2. Transmission Owner that owns a UVLS program

4.3. Transmission Operator that operates a UVLS program

4.4. Distribution Provider that owns or operates a UVLS program

5. Effective Date: April 1, 2005

B. Requirements

R1. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).

R1.1. This assessment shall include, but is not limited to:

R1.1.1. Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.

R1.1.2. Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.

R1.1.3. A review of the voltage set points and timing.

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). (Retired)

C. Measures

M1. Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0_R1.

M2. Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

1.2. Compliance Monitoring Period and Reset Timeframe

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0_R1.1 or an assessment of the UVLS program was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

A. Introduction

1. **Title:** **Under-Voltage Load Shedding Program Performance**

2. **Number:** **PRC-022-1**

3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).

4. **Applicability**

   4.1. Transmission Operator that operates a UVLS program.

   4.2. Distribution Provider that operates a UVLS program.

   4.3. Load-Serving Entity that operates a UVLS program.

5. **Effective Date:** May 1, 2006

B. Requirements

R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UVLS set points and tripping times.

R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.

R1.4. A summary of the findings.

R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. (Retired)

C. Measures

M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.

M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization. (Retired)

D. Compliance

1. Compliance Monitoring Process

   1.1. Compliance Monitoring Responsibility

   Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

2.3. Level 3: Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

2.4. Level 4: Documentation of the analysis of UVLS performance was not provided.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	December 1, 2005	1. Removed comma after 2004 in "Development Steps Completed," #1. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Lower cased the word "region," "board," and "regional" throughout document where appropriate. 4. Added or removed "periods" where appropriate. 5. Changed "Timeframe" to "Time Frame" in item D, 1.2.	January 20, 2006
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Voltage and Reactive Control**

2. **Number:** VAR-001-2

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators.

   4.2. Purchasing-Selling Entities.

   4.3. Load Serving Entities.

5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.

R2. Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

R3. The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.

R3.1. Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.

R3.2. For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.

R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule [1] at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider. (Retired)

[1] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

R6. The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.

R6.1. When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.

R7. The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.

R8. Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.

R9. Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to support its voltage under first Contingency conditions.

R9.1. Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.

R10. Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.

R11. After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

R12. The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

C. Measures

M1. The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule as specified in Requirement 4 to each Generator Operator it requires to follow such a schedule.

M2. The Transmission Operator shall have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3.2.

M3. The Transmission Operator shall have evidence to show that it issued directives as specified in Requirement 6.1 when notified by a Generator Operator of the loss of an automatic voltage regulator control.

M4. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with Requirement 11.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months.

The Compliance Monitor shall retain any audit data for three years.

1.5. Additional Compliance Information

The Transmission Operator shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Violation Severity Levels (no changes)

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	TBD	Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised.
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Exhibit C

Implementation Plan for Project 2013-02

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan
Project 2013-02 – Paragraph 81

Requested Approvals

- None

Requested Retirements

- BAL-005-0.2b R2
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3
- CIP-003-3 R4.2
- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2
- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5
- FAC-011-2 R5
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5

Note that when these Requirements are retired, the version numbers of the standards will NOT be incremented, but the retired Requirements and associated elements will be clearly marked as retired. After evaluating the options and consulting with the Standards Committee and Standards Committee Process Subcommittee, the P81 drafting team determined that this was the most practical approach. Incrementing the version numbers of each standard is impractical because, in some cases, a subsequent version has already been developed. In addition, incrementing the version would require renumbering Requirements where a retired Requirement created a gap in numbering, and this creates an undesirable administrative burden for entities using certain systems to manage their compliance programs.

Prerequisite Approvals

- None

Revisions to Defined Terms in the NERC Glossary

- None

Background

On September 30, 2011, the North American Electric Reliability Corporation (NERC) filed a petition with the Federal Energy Regulatory Commission (FERC) requesting approval of its proposal to make informational filings in a "Find, Fix, Track and Report" (FFT) spreadsheet of lesser-risk, remediated possible violations of Reliability Standards. On March 15, 2012, the FERC issued an order conditionally accepting NERC's FFT proposal. In paragraph 81 (P81) of that order, the FERC stated:

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently. North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, a draft Standards Authorization Request (SAR) was drafted to set forth criteria and a process to identify Reliability Standard requirements that either: (a) provide little protection to the Bulk Electric System; (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file to retire the identified Reliability Standard requirements with appropriate governmental authorities.

Standards Process Input Group (SPIG)

In addition to addressing P81, the SAR was drafted consistent with what the SPIG developed as Recommendation No. 4, as set forth in NERC's Recommendations to Improve The Standards Development Process on page 12 (April 2012), which states:

> Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

Collaborative Process

The draft SAR and a suggested list of Reliability Standard requirements embedded in the SAR for consideration in the Initial Phase was the product of collaborative discussions among the following entities and their members: Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group. The draft SAR was posted for comment, which were due September 4, 2012. The P81 Standards Drafting Team reviewed the comments and finalized the SAR and the proposed list of Reliability Standard requirements for retirement.

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Authority
- Load Serving Entity
- NERC
- Planning Authority
- Planning Coordinator
- Purchasing-Selling Entity
- Regional Entity
- Regional Reliability Organization
- Reliability Coordinator
- Transmission Service Provider
- Transmission Operator
- Transmission Owner
- Transmission Planner

Effective Date of Retirements

All of the Requirements will be retired on the day of approval by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter after approval by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Note that no complete standard is being proposed for retirement and all of the other Requirements in each of the affected standards will remain in continuous effect.

Exhibit D

Consideration of Comments

Project 2013-02
Paragraph 81

Related Files

Status:
Adopted by the NERC Board of Trustees on February 7, 2013 and pending regulatory approval.

Purpose / Industry Need:
This project is in response to paragraph 81 of FERC's March 15, 2012 Order issued on NERC's Find, Fix and Track process. The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES", are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs. Phase 1 of the project identifies Reliability Standard requirements that clearly meet the criteria set forth in the SAR and do not require extensive technical research. Subsequent phases will address Reliability Standard requirements that need additional technical research before retirement or modification.

Draft	Action	Dates	Results	Consideration of Comments
Redline of Standards with Proposed Retirements Implementation Plan **Supporting Materials:** Final SAR Clean | Redline to draft SAR Technical White Paper Redline of VSL Matrix Spreadsheet with Proposed Retirements Comment Form (Word)	Updated Info>> Initial Ballot >>	11/30/12 - 12/10/12 (closed)	Summary>> Full Record>>	
	Join Ballot Pool>>	10/25/12 - 11/23/12		
	Comment Period Info>> Submit Comments>>	10/25/12 - 12/10/12 (closed)	Comments Received>>	Consideration of Comments **(2)**

Proposed SAR Draft SAR Version 1 **Supporting Materials:** Complete Set of Standards with Proposed Retirements for Phase 1 Spreadsheet with Proposed Retirements Comment Form (Word)	Comment Period Info>> Submit Comments>>	08/03/12 - 09/04/12 (closed)	Comments Received>>	Consideration of Comments **(1)**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2013-02 Paragraph 81

The Paragraph 81 Drafting Team thanks all commenters who submitted comments on the Project 2013-02 Paragraph 81 - Retirement of Reliability Standard Requirements. The complete set of standards with proposed retirements for Phase 1 were posted for a 30-day public comment period from August 3, 2012 through September 4, 2012. Stakeholders were asked to provide feedback on the set of standards through a special electronic comment form. There were 43 sets of comments, including comments from approximately 98 different people from approximately 65 companies representing all of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Lee Pedowicz	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Ben Wu	Orange and Rockland Utilities	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Carmen Agavriloai	Independent Electricity System Operator	NPCC	2
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Michael Jones	National Grid	NPCC	1
10.	Donald Weaver	New Brunswick System Operator	NPCC	2

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Michael R. Lombardi	Northeast Utilities	NPCC	1
12.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1
16.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
18.	Brian Robinson	Utility Services	NPCC	8
19.	Michael Schiavone	National Grid	NPCC	1
20.	Wayne Sipperly	New York Power Authority	NPCC	5

2.	Group	Jim Kelley	SERC EC Planning Standards Subcommittee	X				X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Sullivan	Ameren	SERC	1
2.	Bob Jones	Southern Company Services	SERC	1
3.	Pat Huntley	SERC	SERC	10
4.	Darrin Church	TVA	SERC	1

3.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

No additional members listed.

4.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tedd	Snodgrass	WECC	1
2.	Tim	Loepker	WECC	1
3.	Erika	Doot	WECC	3, 5, 6
4.	Alfredo	Bocanegra	WECC	1

5.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Louis Slade		RFC	5, 6
2.	Mike Garton		NPCC	5, 6
3.	Randi Heise		MRO	5, 6
4.	Mike Crowley		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michelle Corley	Cleco Power	SPP	1, 3, 5
2.	Eric Ervin	Westar Energy	SPP	1, 3, 5, 6
3.	Greg Froehling	Rayburn Country Electric Cooperative	SPP	3
4.	Jonathan Hayes	Southwest Power Pool	SPP	2
5.	Louis Guidry	Cleco Power	SPP	1, 3, 5
6.	Bo Jones	Westar Energy	SPP	1, 3, 5, 6
7.	Tiffany Lake	Westar Energy	SPP	1, 3, 5, 6
8.	John Mason	City of Independence, MO	SPP	3
9.	Valerie Pinamonti	American Electric Power	SPP	1, 3, 5
10.	Patrick Smith	Westar Energy	SPP	1, 3, 5, 6
11.	Ashley Stringer	Oklahoma Municipal Power Authority	SPP	4

7.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Godfrey	Pepco Holdings Inc	RFC	1, 3

8.	Group	Jason Marshall	ACES Power Marketing Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 5
2.	Scott Brame	North Carolina Electric Membership Corporation	RFC	1, 3, 4, 5
3.	Bill Watson	Old Dominion Electric Cooperative	SERC	3, 4

9.	Group	Mark S. Gray	The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA)	X		X	X	X	X	X	X		

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			(collectively, the Trade Associations).										
www.eei.org/ for members													
10.	Group	Stephen J. Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda L. Truhe	PPL Electric Utilities Corporation	RFC	1
2.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3
3.	Annette M. Bannon	PPL Generation, LLC on behalf of its Supply NERC Registered Entities	RFC	5
4.			WECC	5
5.	Elizabeth A. Davis	PPL Energy Plus, LLC	MRO	6
6.			NPCC	6
7.			SERC	6
8.			SPP	6
9.			RFC	6
10.			WECC	6

11.	Group	Steve Rueckert	Western Electricity Coordinating Council											X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Phil O'Donnell	WECC	WECC	10
2.	Brent Castagnetto	WECC	WECC	10
3.	Tim Reynolds	WECC	WECC	10
4.	Tyson Jarrett	WECC	WECC	10

12.	Individual	Bob Steiger	Salt River Project	X		X		X	X					
13.	Individual	Al DiCaprio	SRC		X									
14.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X					
15.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X					
16.	Individual	Scott McGough	Georgia System Operations Corporation			X	X							
17.	Individual	Ronnie C. Hoeinghaus	City of Garland	X		X								
18.	Individual	Dan Miller	Entergy Services, Inc.	X		X			X					
19.	Individual	Michael Falvo	Independent Electricity System Operator		X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
20.	Individual	Michelle Clements	Wolverine Power Supply Cooperative, Inc.	X									
21.	Individual	Thomas C. Duffy	Central Husdon Gas & Electric Corporation	X		X							
22.	Individual	John Tolo	Tucson Electric Power	X									
23.	Individual	paul haase	seattle city light	X		X	X	X	X				
24.	Individual	Thad Ness	American Electric Power	X		X		X	X				
25.	Individual	John Seelke	Public Service Enterprise Group	X		X		X	X				
26.	Individual	Jose H Escamilla	CPS Energy	X		X		X					
27.	Individual	Laura Lee	Duke Energy	X		X		X	X				
28.	Individual	Rich Salgo	NV Energy	X		X		X					
29.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
30.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
31.	Individual	Michelle R. D'Antuono	Occidental Energy Ventures Corp.			X		X		X			
32.	Individual	Patrick Brown	Essential Power, LLC					X					
33.	Individual	Becky Stewart	Idaho Power Company	X		X							
34.	Individual	Kimberly Tolbert	Occidental Power Services, Inc.			X							
35.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
36.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
37.	Individual	Eric Olson	Transmission Agency of Northern California	X									
38.	Individual	Kirit Shah	Ameren	X		X		X	X				
39.	Individual	Jason Snodgrass	Georgia Transmission Corporation	X									
40.	Individual	Kristin Iwanechko	NERC Staff Technical Review										
41.	Individual	Cheryl Moseley	Electric Reliability Council of Texas, Inc.		X								
42.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				
43.	Individual	Judy VanDeWoestyne	MidAmerican Energy Company	X		X		X	X				

1. **Do you agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement? If not, please explain in the comment area.**

Summary Consideration:[2]

The majority of commenters supported the Criteria A, B and C included in the draft SAR, with a few commenters suggesting changes.

A. Comments on Criterion A

The P81 standards drafting team (P81 SDT), in conjunction with NERC's technical staff review, believes it is appropriate to rephrase Criterion A to be similar to Criterion B 9, which comports with the FFT Order, and, at the same time, to eliminate Criterion B 8 and Criterion B 9 to avoid any confusion between Criterion A and Criterion B. The P81 SDT believes the following provides a more suitable overarching Criterion A:

"The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES."

Comments

The Western Electricity Coordinating Council (WECC) and Northeast Power Coordinating Council (NPCC) requested clarification or alternative wording of Criterion A, while Independent Electricity System Operator and NPCC also saw Criterion A and Criterion B 9 as redundant or duplicative. Manitoba Hydro also believed there was a need to clarify Criterion B 9 and Occidental Energy Ventures Corp. desires that Criterion A implicate Section 215 of the Federal Power Act, while Occidental, like others, also believes Criterion B 8 and Criterion B 9 need clarification.

Response

The P81 SDT believes the above revision of Criterion A and elimination of Criterion B 8 and Criterion B 9 addresses the commenters' concerns, while still including the Section 215 term reliable operation.

B. Comments on Criterion B

[2] Although responses to informal comments are not required in the detail found in the P81 SDT responsive comments, the P81 SDT believed it was appropriate to provide more detail given the level of interest in this Standards Development Project. The format and detail of these responses are not precedent setting with respect to how other SDTs respond to an informal comment period.

Comment

WECC states it only agrees with Criterion B 1 if each administrative requirement meets all the sub-requirements listed (administrative in nature, does not support reliability and needlessly burdensome). In addition, ACES Power Marketing Standards Collaborators states that in Criterion B 1 it would be best to strike "and is needlessly burdensome."

Response

The list of requirements was meant to apply to each candidate and uses the term "and" not "or" to ensure all three are required. The wording of Criterion B 1 was carefully considered in the collaborative process, and it was believed that the current wording, which tends to match with WECC's understanding, is appropriate. Thus, the P81 SDT believes that no changes to Criterion B 1 are necessary.

Comment

WECC disagrees with Criteria B 3, B 4 and B 5 unless it may be demonstrated that there is no benefit to reliability at all.

Response

WECC's comment seems misaligned with FERC's intention which the P81 SDT believes was for NERC and stakeholders to investigate what requirements provide little protection to the BES, are unnecessary or redundant. WECC's approach seems much stricter and seems to suggest that if any plausible argument can be made, the requirement cannot be retired. Such an argument is not in line with the rest of the commenters and, therefore, will not be adopted. In addition, as the project proceeds through the standard drafting process, sufficient technical justifications will be put forward for industry review for each proposed requirement for retirement. The industry will have further opportunity to evaluate the technical justifications as the P81 project moves forward.

Comment

SRC believes that the SAR captures the right categories, but states that Criteria B 2 through B 5 could be sub-items of B1. In a similar light, NERC staff states there is significant overlap between Criterion B 3 (Purely Documentation) and Criterion B 5 (Periodic Updates) and these criteria could be combined. Independent Electricity System Operator and SRC also disagree with Criterion B 5.

Response

While annual reviews may be necessary, there may be other ways to ensure periodic reviews are done. Criterion B 5 was contemplated by the P81 SDT more in the context of future phases which would allow for the modification of requirements, not an easily identified retirement. Thus, while to some extent we share the concerns of SRC, NERC staff and Independent Electricity System Operator, we believe that the use of Criterion B 5 may be useful in facilitating review of further requirements by the stakeholders.

Comment

WECC disagrees with the use of Criterion B 2 because data and evidence collection is necessary to demonstrate compliance.

Response

The P81 SDT believes that this concern appears to miss the essential aspect of the P81 project in its initial phase which is to retire requirements that do little to protect BES reliability. Thus, hardwiring in data retention mandatory requirements does not seem aligned with generally accepted methods of auditing or promoting an effective and efficient ERO. It is incumbent on the entities to maintain sufficient evidence to support compliance with requirements, and the P81 SDT believes that any requirements that strictly support compliance assessments without a benefit to reliability should be evaluated for revision or retirement.

Comment

WECC disagrees with Criterion B 7 because it would allow other regulators to enforce a requirement.

Response

The P81 SDT agrees with WECC's overarching concern; however, that situation exists today. If there is a requirement that is already part of a regulatory order or under the purview of another governmental authority and is consistently understood and applied across North America, then the P81 SDT believes it should remain a candidate for retirement to remove this potential for double jeopardy. It is important to note, however, that it must be consistently covered across the whole continent and mandatory so as to ensure no "gaps" exist.

Comment

Independent Electricity System Operator suggests that another word be used other then "Technical" to describe Criterion B.

Response

Based on this concern, the P81 SDT changed "Technical" to "Identifying."

C. <u>Comments of Criterion C</u>

Comment

WECC believes Criterion C 1, C 2, C 4, C 6 and C 7 all need to be made more specific or improved.

Response

The concern seems predicated on Criterion C determining whether or not to retire a requirement, which is not the intent. Instead, these criteria will be used to ensure additional pertinent information and considerations are used to assist in the determination of whether a Reliability Standard requirement satisfies both Criterion A and Criterion B. The P81 SDT shall consider these data and

reference points to make a more informed decision. Also, note that these criteria are conceptual only and were developed to assist the industry and the P81 SDT with their analysis. The P81 SDT thanks WECC for their thorough review; however, it will retain the criteria as written.

Comment

Independent Electricity System Operator states it is confusing as to how the section C, "Additional Data and Reference Points" will be used by the drafting team to determine retirement of Reliability Standards even though they have satisfied Criterion A and Criterion B.

Response

The P81 SDT believes that a review of the technical white paper, which will be issued and will contain the initial list of requirements to be retired, will promote an understanding on how Criterion C was used. Criterion C is only meant to provide additional considerations to provide further justifications that the proposed retirements do not have any other underlying reliability related need.

D. Miscellaneous Comments on Phase I vs. Subsequent Phases

Comment

ACES Power Marketing Standards Collaborators suggest that the scope of the SAR should be changed to include current standards under development.

Response

At this time it appears that including requirements from current standards under development would overly complicate the P81 project and intrude on other standard drafting teams. With that said, the P81 SDT does intend to work with and coordinate with other standard drafting teams to help ensure that new requirements are not being drafted that appear to meet the P81 criteria. Also, the P81 SDT will be working with the Standards Committee to draft guidelines to help standard drafting teams draft requirements that are more results-based, and not requirements that would meet the P81 criteria.

Comment

ERCOT indicates that the criteria used for future phases should remain flexible.

Response

The initial list should not preclude the use of additional criteria for future phases where additional criteria support the elimination of requirements in those efforts. Given the amount of commenters who requested numerous requirements be considered in future phases, it appears reasonable that P81 project should remain flexible to meet the needs of stakeholders. Thus, the P81 SDT has revised the SAR to apply to Phase I only.

Comment

SRC urges the SAR simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired.

Response

The P81 SDT did not intend for the list of requirements proposed in the draft SAR to come across as a list without flexibility.

Comment

ACES Power Marketing Standards Collaborators suggests that requirements that are assigned to the wrong functional entities should be added as a criterion for revision or retirement.

Response

The P81 SDT believes that ACES's suggestion should be considered during the development of a Phase 2 SAR. In many instances, applicability can be a complex undertaking and there may be large diversity, irrespective of an entity having some common high-level responsibilities as listed in the NERC Registry and Functional Model.

Comment

NERC staff suggests that any technical justifications that rely on Criterion B 6 should address how NAESB, etc. would handle the requirement.

Response

As a general matter, many commenters suggest that the P81 project develop thorough justifications and remain in line with the suggested Criteria. NERC staff's concern of reliance on Criterion B 6 will also be considered when developing the justifications. The P81 SDT removed references to NAESB, but notes that when relying on B 6, sufficient reference will be made to other mandatory requirements which effectively ensure there will be no gap on a continent-wide basis and in addition, what will ensure that on an ongoing basis, this gap will remain addressed by something other than a NERC standard requirement. The technical white paper will consider these concerns. In addition, the P81 SDT believes that ongoing training for drafting teams will ensure that these types of requirements are no longer developed.

Organization	Yes or No	Question 1 Comment

Organization	Yes or No	Question 1 Comment
Western Electricity Coordinating Council	No	WECC offers the following related to the criteria listed in the SAR.WECC beleives the OVERARCHING CRITERIA listed under "A" needs clarification and that as currently identified is too vague. The Overarching Criterion statement is too broad and is contrary to the FPA Section 215. "Impact" is an ambiguous term. There is no measure as to how to quantify a Requirement's "impact" and to distinguish between "little" impacts as opposed to some other metric of "impact." More importantly, however, a Requirement that has any impact on the reliable operation of the BES cannot be dismissed as inconsequential, even if it is determined to have "little" impact. The "impact" must be weighed against the "burden" of the standard and potential for efforts to demonstrate compliance hindering or preventing other more "impactful" reqiurements. Further, the Standard Requirements work in concert with one another. For many Standard Requirements, it is impossible to reasonably assess the "impact" of a single Standard Requirement. For example, the "purpose" statement for CIP Standard Requirements reads that "[CIP Standard Requirements] should be read as part of a group of standards numbered Standards CIP-002 through CIP-009." To examine the "impact" of a single Standard Requirement, therefore, contradicts the intent and purpose of many Standard Requirements that are crafted to operate in concerns with one another.WECC believes the B1 Administrative Technical Criteria needs claificaiton and is vague as currently written. The term "administrative" is ambiguous and could cover a broad range of activities. Further, "administrative requirements" often require evidence of program or procedure creation. However, WECC does agree with this criteria, but only in the case where all three criteria listed (administrative, does not support reliability, and needlessly burdensome) are met.WECC disagrees witht he B2 Technical Criteria Data Collection/Data Retention. Data Collection/Data Retention is often the only means by which a Responsible Entity can objectively demonstrate compliance. As to mandatory data retention

Organization	Yes or No	Question 1 Comment
		periods, an explicit mandate to retain data may be required to meet compliance obligations unique to a particular Standard Requirement. However, if treated correctly, a requirement for the data collection/retention for compliance purposes could be removed from the Requirmeetns and made part of the Measures or RSAWs.WECC Disagrees with the B3 criteria Purley Documentation unless it can be clearly demonstrated that the dcoumentation does not protect the reliabiltity of the BES in any way. In some cases Plans/Policies/Procedures are necessary for employees to have a guide for not only protection but maintaining and restoring BES assets (i.e. Restoration Plans). Documentation of plans, policies and procedures, is key in defining the parameters of compliance. Further, plans/policies and procedures are often the only means by which Compliance and Enforcement can assess a responsible entity's compliance with a Standard Requirement.WECC Disagrees with the B4 criteria Purely Reporting unless no purpose for the reporting can be identified. Reporting helps overarching organizations (ex. ES ISAC) detect potential issues earlier, by giving them more information and from multiple entities. These issues may seem small or insignificant when viewed by a singular entity but may have a more a drastic impact when viewed from the perspective of the entire BES. WECC Disagrees with the B5 criteria Periodic Updates unless it can be clearly demonstrated that the reproting has no operational benefit to reliability. Without these requirements there is nothing in place to ensure entityies are maintaining, and periodically verifying the accuracy of these documents. With the criteria established as it is, there is no real way of measuring the effect of "operational benefit to reliability". Is it measured by the size of impact (MW), by time (something that will take over a 1hr), or by Time Horizon (Same-Day operations vs. Real Time Operations). It is recommended to establish a more accurate means to measure these criteria. If proberly handled, these reporting requirements that that demonstrate the entities are maintaining certain necessary

Organization	Yes or No	Question 1 Comment
		documents could be moved from the Requirements to the Measures or RSAWs.WECC agrees with the B6 criteria of Business Practices.B7 criteria Redundant: Although WECC agrees requirements should not be redundant with each other, if compliance is left to other regulators (Open Access Transmission Tariff, NAESB, etc.) compliance may not be held up to NERC expectations or interpretations. In identifying redundant standards, only NERC Reliability Standards should be considered.WECC agrees with B* criteria,WECC believes the B9 criteria needs clarification and as written is vague. How will the determination that teh Requirements do little, if anything, to promote the protection of the BES be determined?WECC disagrees with C1. The FFT determination is not predicated on any particular Standard Requirement. The FFT determination is fact specific. Even a requirement that is critical to the BES may have an FFT'd violation if the manner in which the requirement was violated was minor.WECC beleives C2 is vague and needs clarification. Not certan what it means if the requirement is being revieweed in an on-going Standards Development Project. Is this the same as B7 Redundant?WECC agrees C3 is a factor that should be considered.WECC agrees with C4 but beleives information on how the tiers will be viewed should be included.WECC agrees with C5.WECC believes C6 and C7 are vague as written and believes that these last two reference points are intended to indicate that if the answer is yes, then the requirement or standard would NOT be eligable for retirement. This should be clarified.
Independent Electricity System Operator	No	(1) The IESO supports this proposed effort and agrees with most of the criteria, with some exceptions (except #5): "The Reliability Standard requirement requires responsible entities to periodically update (e.g., annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability."Take for example the system restoration plan. An annual review is necessary to ensure that the plan recognizes BES facility changes that occurred since the last review/update. Another

Organization	Yes or No	Question 1 Comment
		example is the exceptions to the cyber security policy that needs to be reviewed and approved by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Applying this criterion in a broad brush manner without looking at each requirement may result in removing requirements that are still needed for reliability.(2) Generally, the nine criteria listed in the SAR are simple and sufficient to be used to determine retirement of reliability standard requirements. It is recommended that the word "Technical" in the heading of the B section "Technical Criteria" be erased as the criteria aren't based on technical data. Also, it is unclear and confusing as to how the section C "Additional Data and Reference Points" will be used by the drafting team to determine retirement of reliability standards even though they have satisfied Criteria A and B. Criterion B.9 can potentially be deleted as its purpose seems to be the duplication of Criterion A.(3) The SAR narrative for TOP-001-1a R3 states the requirement is redundant with IRO-001-1a R8. IRO-001-1a does not exist; we believe, it should be IRO-001-1.1 R8 instead.
NERC Technical Staff Review	No	(1) Revise Criteria A to focus on the content of the Reliability Standards. NERC Staff suggests the following language for Criteria A: "The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to protect reliable operation of the BES." This language is currently included as Criteria B9. NERC notes that both Criterion B8 (hinders the protection or reliable operation of the BES) and B9 (little, if any value as a reliability requirement) are duplicative with Criterion A and should be eliminated. Since any requirement that meets Criterion B8 or B9 would necessarily meet Criterion A, this creates an unintended consequence by undermining the objective that requirements for consideration must satisfy both the overarching Criterion A and a separate technical criteria. For these reasons, NERC Staff supports the elimination of both Criteria B8 and B9 and the re-phrasing of Criteria A. (2) There is significant overlap between Criteria B3 (Purely Documentation) and B5

Organization	Yes or No	Question 1 Comment
		(Periodic Updates) and these criteria could be combined. Criteria B3 addresses requirements for entities to develop a document that is not necessary and Criteria B5 addresses the requirement for entities to periodically update such documentation. NERC Staff suggests renaming Criteria B3 "Documentation" and suggests the following language: "The Reliability Standard requirement requires responsible entities to develop and/or periodically update a document (e.g., plan, policy or procedure) which is not necessary to protect BES reliability." (3) The explanation of Criterion B6 (Commercial or Business Practice) states that the Reliability Standard requirement "is a commercial or business practice, e.g., better served as a NAESB standard or as part of NAESB Electric Industry Registry (EIR)." However, the technical justifications provided for the application of the B6 criteria do not state that the standard/requirement should be addressed in another manner, e.g., with a NAESB standard. Please clarify or otherwise modify this criterion appropriately. Further, the technical justification should address the fact that such business practices may not be applicable to the same entities and may not be mandatory or enforceable.
Northeast Power Coordinating Council	Yes	NPCC participating members support the P81 initiative and agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement. The criteria are also consistent with FERC's guidance in Paragraph 81 of the FFT Order. With respect to the words in Criterion A wording, it could be interpreted as an indication that the original reliability standard requirement was a mistake. Suggest the SDT consider alternative wording to indicate that the experience with the requirement, over time, has proven not to be useful to accomplish its initially intended reliability objective, or has not produced clear results for the initially intended reliability objective.Criterion A, and Technical Criteria B9 "Little, if any, value as a reliability requirement" are redundant.

Organization	Yes or No	Question 1 Comment
ACES Power Marketing Standards Collaborators	Yes	In general, we agree with the criteria. However, we do offer two suggestions. First, in criterion B.1, we suggest striking "and is needlessly burdensome". If the activity does not support reliability the burden is irrelevant. Second, we suggest if there are current standards under development that are already proposing to retire requirements that those requirements should be considered for inclusion in this project. In order to include those requirements, the proposed reason for retirement should align with one of the criteria in this project. This would accelerate the retirement of unnecessary requirements. Third, we suggest requirements that are assigned to the wrong functional entities should be added as a criterion for revision/retirement.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade Associations).	Yes	The Trade Associations agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement. As noted above, the criteria were the product of intense discussions among numerous stakeholders, including the Trade Associations, NERC, and the Regional Entities. The criteria are also consistent with FERC's guidance in paragraph 81 of the FFT Order.
SPP Standards Review Group	Yes	We concur that the proposed criteria are a good starting point for the evaluation of requirements to be retired.
Salt River Project	Yes	We like the criteria and methodology.

Organization	Yes or No	Question 1 Comment
SRC	Yes	The criteria listed in the SAR capture the right categories; however, consider restructuring B1. B2 through B5 are examples of administrative requirements and should possibly be sub-items of B1. While we generally support this proposed effort and agrees with most of the criteria, the exception is B5: “The Reliability Standard requirement requires responsible entities to periodically update (e.g., annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.”Take for example the system restoration plan. An annual review is necessary to ensure that the plan recognizes BES facility changes that occurred since the last review/update. Another example is the exceptions to the cyber security policy that needs to be reviewed and approved by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Applying this criterion in a broad brush manner without looking at each requirement may result in removing requirements that are still needed for reliability. In addition, the acid test for retirement of a requirement is when the standard drafting team reviews the overall reliability impact of removing a particular requirement from a standard, and how it may affect other related standards. In brief, it may be a bit premature to pass on this judgment at the SAR stage. We urge the SAR proponent to simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired. And, in order to meet the requirements for regulatory approval, we suggest the SDT to provide strong technical basis to justify each retirement.
Manitoba Hydro	Yes	The technical criteria B.9, "Little if any, value as a reliability requirement", is very subjective and should be redefined or clarified.
Georgia System Operations Corporation	Yes	Georgia System Operations agrees with the criteria listed in the SAR to identify Reliability Standard requirements for either modification or

Organization	Yes or No	Question 1 Comment
		withdrawal.
seattle city light	Yes	Seattle City Light supports the consolidated comments of the industry Trade Organizations.
NV Energy	Yes	We agree with the Overarching Criterion and the specific Technical Criteria, and believe that the types of requirements specified in the Technical Criteria can be eliminated without any impact to reliable operation of the interconnected transmission system.
Occidental Energy Ventures Corp.	Yes	Occidental Energy Ventures Corp. ("OEVC") fully supports the efforts taken by the Trades, NERC, and the Regional Entity Management Group to develop the criteria to identify requirements that may be eligible for retirement and modification. The overarching criterion is extremely important in our view, as it serves to remind us all that FERC's original purpose as defined by Section 215(a)(4) of the Federal Power Act is to oversee wide-area reliability of the bulk power system. In recent years, the Commission's authority has expanded into distribution systems and localized load shedding - important issues, but already regulated by the PUCs. In our view, this is duplicative work that increases costs without serving improved reliability.OEVC also believes that the technical criteria are appropriate and complete for now. However, in our view, Item #8 "Hinders the protection or reliable operation of the BES" and Item #9 "Little, if any, value as a reliability requirement" will need further refinement in future phases of this project. Both are quite subjective, and FERC in our opinion will only respond to fact-based quantitative data that shows that BPS reliability is not improved by a given reliability requirement. A painful reminder may be the requirement for secondary Facility Ratings (FAC-008-3) which FERC clearly perceives to be a reliability imperative despite overwhelming industry rejection of the concept. It is unlikely that this view will change unless tangible cost/benefit evidence to the contrary

Organization	Yes or No	Question 1 Comment
		is provided to the Commission.
South Carolina Electric and Gas	Yes	I support removing redundancy and any items that are not related to reliability impacts.
Georgia Transmission Corporation	Yes	Georgia Transmission Corporation agrees with the criteria listed in the SAR to identify Reliability Standard requirements for either modification or withdrawal.
Electric Reliability Council of Texas, Inc.	Yes	ERCOT agrees with the ISO/RTO SRC comments. However, in addition for SRC comments, ERCOT offers the following: ERCOT agrees with the criteria listed in the SAR to identify Reliability Standard requirements for retirement in Phase 1. However, the criteria used for future phases should remain flexible. The initial list should not preclude the use of additional criteria for future phases where additional criteria support the elimination of requirements in those efforts.
SERC EC Planning Standards Subcommittee	Yes	
Southwest Power Pool Regional Entity	Yes	
Bonneville Power Administration	Yes	
Dominion	Yes	
Pepco Holdings Inc & Affiliates	Yes	
PPL Corporation NERC Registered Affiliates	Yes	

Organization	Yes or No	Question 1 Comment
Tampa Electric Company	Yes	
City of Garland	Yes	
Entergy Services, Inc.	Yes	
Wolverine Power Supply Cooperative, Inc.	Yes	
Central Husdon Gas & Electric Corporation	Yes	
Tucson Electric Power	Yes	
American Electric Power	Yes	
Public Service Enterprise Group	Yes	
CPS Energy	Yes	
Duke Energy	Yes	
Edison Mission Marketing & Trading	Yes	
Illinois Municipal Electric Agency	Yes	
Essential Power, LLC	Yes	
Idaho Power Company	Yes	
Occidental Power Services, Inc.	Yes	

Organization	Yes or No	Question 1 Comment
City of Austin dba Austin Energy	Yes	
Transmission Agency of Northern California	Yes	
Ameren	Yes	
Kansas City Power & Light	Yes	
MidAmerican Energy Company	Yes	

2. The Initial Phase of the P81 project is designed to identify all FERC-approved Reliability Standard requirements that easily satisfy the criteria. Do you agree that the suggested list of Reliability Standard requirements included in the draft SAR easily satisfy the criteria listed in the draft SAR? If you disagree, please provide a statement supporting what Reliability Standard requirements you would add or subtract from the Initial Phase, including a citation to at least one element of Criterion B, as applicable.

Summary Consideration:

A. Support for Initial List

The majority of commenters support the initial list of requirements suggested for retirement in the draft SAR. Supporters include SPP Standards Review Group, The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC), the Canadian Electricity Association (CEA) (collectively, the Trade Associations), Salt River Project, SRC, Georgia System Operations Corporation, Seattle City Light, Duke Energy, NV Energy, Occidental Energy Ventures Corp., South Carolina Electric and Gas, Ameren, Electric Reliability Council of Texas, Inc., SERC EC Planning Standards Subcommittee, Dominion, Pepco Holdings Inc & Affiliates, PPL Corporation NERC Registered Affiliates, Tampa Electric Company, Manitoba Hydro, City of Garland, Entergy Services, Inc., Wolverine Power Supply Cooperative, Inc., Central Hudson Gas & Electric Corporation, Tucson Electric Power, CPS Energy, Edison Mission Marketing & Trading, Illinois Municipal Electric Agency, Idaho Power Company, City of Austin dba Austin Energy, Transmission Agency of Northern California, and Kansas City Power & Light. Also, the following entities appear to generally support the current list, while requesting additional requirements to be added: Georgia Transmission Corporation, Occidental Power Services, Inc., American Electric Power, and ACES Power Marketing Standards Collaborators. This level of support appears to be a testament to the hard work of the collaborative process and provides significant context in which to consider the merits of those stakeholders who requested that certain requirements be added or removed from the initial list.

B. Concerns with requirements included in the initial list

Comment

Northeast Power Coordinating Council (NPCC), Southwest Power Pool Regional Entity (SPP RE), Western Electricity Coordinating Council (WECC), NERC staff technical review (NERC staff) presented concerns with retiring requirements related to PRC-008-0 and PRC-009-0.

Response

As SRC points out, PRC-009-0 is already scheduled to be retired. More specifically, in Order No. 763 at Paragraph 103[3] the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Similarly, under Standards Development Project 2007-17 Protection System Maintenance, which recently passed stakeholders vote on August 27, 2012, PRC-008-0 is scheduled to be retired and replaced with PRC-005-2. PRC-005-2 will likely be presented to the NERC Board of Trustees in November for approval. To avoid confusion and promote regulatory efficiency, the P81 SDT intends to present PRC-008-0 and PRC-009-0 in the final SAR for informational purposes only. Accordingly, PRC-008-0 and PRC-009-0 will not be included in the P81 project for purposes of comment and ballot.

Comment

NPCC is concerned that it may only receive information related to UVLS program assessment and performance after an event if PRC-010-0 R2 and PRC-022-1 R2 are retired.

Response

The P81 SDT believes it is appropriate to retire PRC-010-0 R2 and PRC-022-1 R2 because the Regional Entities' current compliance and monitoring processes provide for the review of UVLS program assessment and performance during a spot check, compliance audit, etc., which makes PRC-010-0 R2 and PRC-022-1 R2 unnecessary. Thus, the P81 SDT believes that PRC-010-0 R2 and PRC-022-1 R2 should remain within the scope of P81 for purposes of comment and ballot.

Comment

WECC and SPP RE requested that CIP-007-3 R7.3 not be retired, based on concerns related to demonstrating compliance with other requirements.

Response

These concerns appear to miss the essential aspect of the P81 project which is to retire requirements that do little to protect BES reliability. The P81 SDT believes that data retention in and of itself has little to do with protecting BES reliability, particularly when the Regions have authority to request data to show compliance with any mandatory Reliability Standard. Thus, hardwiring in data retention into mandatory Reliability Standard requirements does not seem aligned with generally accepted methods of auditing or promoting an effective and efficient ERO compliance program. In other words, it seems to adopt the position of WECC and SPP RE on this matter could essentially be an endorsement that every Reliability Standard requirement should be accompanied with a mandatory data retention requirement, which would seem counterintuitive given the processes set for in the Compliance Monitoring and Enforcement Program. Thus, the P81 SDT believes that CIP-007-3 R7.3 should remain within the scope of P81 for purposes of comment and ballot.

[3] *Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards*, 139 F.E.R.C. ¶ 61,098 (2012).

Comment

WECC also disagrees with the inclusion of IRO-016-1 R2 with a concern that Reliability Coordinators must be required to document their actions for compliance and enforcement purposes.

Response

Reliability Coordinator actions are conducted over recorded lines or via written directives, and, thus, the documentation is already available for a Regional Entity to inspect. Further, during a spot check or compliance audit a Regional Entity has the authority to request information, as well as the entity has the burden to prove compliance – if the entity chooses to prove compliance via recorded phone lines or logs is not necessarily an appropriate subject for a mandatory Reliability Standard. Thus, the P81 SDT believes that IRO-016-1 R2 should remain within the scope of P81 for purposes of comment and ballot.

Comment

WECC and NERC staff express concerns with including MOD-004-1. Specifically, WECC states:

MOD-004 is not redundant to TOP-002 even though the CBM itself may be a tariff issue and rarely used. The reliability piece is that if the CBM is used by a TSP then the details of it must be available for use in system studies. Without the awareness of a transmission holdback for CBM when it exists, a network study could be run and show no issues but if at some time the CBM were implemented an overload could result. This might not always be the case but unless the CBM parameters are known and modeled it could impact reliability.

NERC staff suggests that MOD-004-1 may be more appropriate for a subsequent phase unless a solid technical justification can be developed for MOD-004-1 that addresses relevant FERC's ruling.

Response

One of the tenants of the initial phase of P81 is that the requirement does not need significant technical justifications or editing. Notwithstanding the apparent support for MOD-004-1 to be part of the P81 project, it is also apparent to the P81 SDT that at this time MOD-004-1 needs additional review and consideration prior to any decision to retire all or part of its requirements. It is also noteworthy that there are a large number of requests to consider other MOD standards in subsequent phases, and it is likely appropriate to consider the MOD Standards as a whole so that MOD-004-1 can be more thoroughly analyzed. For example, CBM is referenced in a number of MOD Standards, such as MOD-001-1a, MOD-008-1 and MOD-028-1. Thus, the P81 SDT has removed MOD-004-1 from the list of requirements proposed for the initial phase and MOD-004-1 will be considered in a subsequent phase of the P81 project.

Comment

WECC, Public Service Enterprise Group and Essential Power, LLC state that CIP-002-1a R4 should not be retired. WECC makes several points, including:

"An entity has many enforcement agencies to contact without the FBI listed in the operating instructions they could easily be overlooked. . . . . Retiring R4 will remove the incentive of having a working relationship with the FBI, especially among the smaller entities. Retiring R4 may effectively delay or prevent the FBI from rapidly locating those responsible for sabotage."

Also, Public Service Enterprise Group and Essential Power, LLC state:

"If the entity owns or operates a BES asset, there is a clear reliability benefit to have appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to these Law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response."

Response

The P81 SDT believes that the practices and procedures discussed by WECC, Public Service Enterprise Group and Essential Power, LLC are accomplished via R1 through R3 of CIP-002-1a, not R4. For example, consistent with R2,[4] it is common practice to contact local law enforcement authorities when there is any suspicion that sabotage has occurred at a BES facility. The entity's corporate security and site personnel will consult with local law enforcement to assess the situation and facts to determine whether a suspected or actual act of sabotage has occurred. If they find a suspected or actual act of sabotage has occurred, reliability entities as well as the Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP), as appropriate, will be contacted in accordance with R2. Thus, pursuant to R1 through R3, when there is an instance of sabotage that warrants contacting the FBI or RCMP or any other federal or national governmental authority, entities will contact them. Conversely, the requirement in R4 to establish communication contacts with the FBI or RCMP, as applicable, is purely an administrative, documentation and data collection task requirement – there is no operational or results-based aspect of R4, like there is with R1 through R3. Accordingly, in CIP-001-2a R1 through R3 serve the results-based reliability function, while R4 is a static, administrative requirement that has no direct or clear nexus to protecting BES reliability. For these reasons, the P81 SDT believes that CIP-001-2a R4 should remain within the scope of P81 for purposes of comment and ballot.

Comment

Bonneville Power Administration, WECC and NERC staff do not support the proposed retirement of TOP-001-1a R3.

[4] "**R2.** Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection."

Response

Bonneville Power Administration, WECC and NERC staff all make valid points. Although there is redundancy between TOP-001-1a R3 and IRO-001-1a R8 related to Reliability Coordinators, this redundancy was addressed in Standards Development Project 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces TOP-001-1a R3 and reads as follows:

Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued and identified as such by its Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.

TOP-001-2 has been approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, the P81 SDT intends to present TOP-001-1a R3 in the final SAR for informational purposes only. Accordingly, TOP-001-1a R3 will not be included in the P81 project for purposes of comment and ballot.

Comment

SRC and NERC staff state that VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2 should not be included in the P81 project until they have first been processed for retirement via the WECC regional standards process.

Response

SRC and NERC staff make a valid point that regional standards proposed for retirement need to first proceed through their region prior to being considered for retirement via a NERC standards development project. For these procedural concerns, VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2 have been removed from the P81 project; however, the P81 SDT encourages WECC to consider the deliberations of the collaborative process and act on retiring VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2, as appropriate.

Comment

Central Hudson Gas & Electric Corporation, Public Service Enterprise Group, and American Electric Power and Essential Power, LLC express concern with the inclusion of CIP-003-3 R4 and its sub-requirements in the P81 project. AEP states:

“AEP recommends instead that CIP-003 R1 be removed in which case CIP-003 R3 (and CIP-003 R2.4) can also be removed. However, if the drafting team does not agree with this recommendation, CIP-003 R3 must be retained in order for entities to take targeted exception(s) where applicable (for example, in circumstances where an entity’s program is more stringent than the CIP requirements).”

Public Service Enterprise Group and Essential Power, LLC indicate that “[t]he exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy.”

Response

The reason for retiring CIP-003-3, -4 R3 and its sub-requirements is directly applicable to the concerns expressed. In other words, although the CIP exception requirements have never been available for use to exempt an entity from compliance with any requirement of any NERC Reliability Standard, entities apparently are reading the CIP exception requirements out of context. These requirements only apply to exceptions to internal corporate policy, and only in cases where the policy exceeds a NERC Reliability Standard requirement or addresses an issue that is not covered in a NERC Reliability Standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of eight characters in length, and be changed every 30 days, this provision could be used for internal governance purposes to lessen the corporate requirement back to the password requirements in CIP-007 R5.3, or in conjunction with a Technical Feasibility Exception (TFE) to something else. Therefore, removal of this requirement has no effect on the TFE process or compliance with any other CIP requirement. Also, the retirement of the CIP exception requirements would not impact an entity's ability to maintain such a process within their corporate policy governance procedures. Consequently, the CIP exception requirements provide little protection for BES reliability and are an internal administrative and documentation requirement that is outside the scope of the other CIP requirements. Thus, the P81 SDT believes that CIP-003-3, -4 R3 and its sub-requirements should remain within the scope of P81 for purposes of comment and ballot.

Comment

Public Service Enterprise Group and Essential Power, LLC also request the P81 project not include EOP-004-1 R1 because it will soon be replaced by EOP-004-2.

Response

The P81 SDT notes that the past ballot of EOP-004-2 did not pass and it is currently in the balloting stage. The P81 SDT has coordinated its efforts with the chair of Project 2009-01 and both agree there is no conflict between retiring EOP-004-1 R1 and the direction of Project 2009-01. At such time that the EOP-004-2 project does obtain stakeholder approval and is scheduled for NERC Board of Trustees review, P81 SDT will reconsider the need to include EOP-004-1 R1. Thus, at this time, the P81 SDT believes that EOP-004-1 R1 should remain within the scope of P81 for purposes of comment and ballot.

Comment

Public Service Enterprise Group and Essential Power, LLC further request that FAC-002-1 R2 be removed from the P81 project based on the concern that the three year study retention requirement could be increased to six years via compliance and monitoring data retention.

Response

The concern of Public Service Enterprise Group and Essential Power, LLC, however, appears to miss the essential aspect of the P81 project in its initial phase which is to retire requirements that do little to protect BES reliability. Thus, hardwiring in data retention

mandatory requirements does not seem aligned with generally accepted methods of auditing or promoting an effective and efficient ERO compliance program. Accordingly, the P81 SDT believes that FAC-002-1 R2 should remain within the scope of P81 for purposes of comment and ballot.

Comment

NERC staff questioned the inclusion of FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 in the P81 project. Specifically, NERC staff states:

"These requirements, combined with others, provide checks and balances on the Facility Rating Methodology and Transfer Capability methodology established by the responsible entities. This provides a reliability benefit by requiring the responsible entity to consider areas in which their methodology may not be sufficient to support reliable operation of the interconnected transmission system. There may be better ways of assuring that entities have sufficient methodologies and alternatives should be considered during Phase II. NERC Staff suggests that the SDT reconsider whether discussing the methodology (and not the numerical rating of a facility) has commercial or market related implications. With respect to FAC-013-2 R3, NERC Staff suggests that the SDT reconsider whether the requirement relates to "a back and forward on transfer capability" as noted in the draft SAR, as the requirement pertains only to the methodology for determining transfer capability."

Response

The P81 SDT notes that Page 5 of NERC's Standards Process Manual states:

"A Reliability Standard includes a set of Requirements that define specific obligations of owners, operators, and users of the North American Bulk Power Systems. The Requirements shall be material to reliability and measurable."

It appears difficult to read into the plain language of FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 specific obligations that are material to reliability and measurable or provide more than a little amount of protection to BES reliability. For instance, in practice, while the owners of ratings and transmission capability methodologies have made these documents available for comment during the duration of the mandatory Reliability Standard regime, experience shows that little, if any, technical comments have not been submitted on these documents. In the regional processes, entities are on a variety of committees and have professional relationships, and, therefore, if they have a concern with a methodology, they have ample opportunity to seek out professional technical critique as a best practice. FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 seem toonly formalize a vehicle for professional technical critique without an exacting nexus between it and reliability. Given that entities that develop these methodologies must comply with rigorous requirements in FAC-008 and FAC-013, the P81 SDT believes that the addition of a mandatory best practice technical critique process does not seem necessary, material or measurable. It is also noteworthy that there is no obligation for any entity to request a methodology nor is there any obligation on the owner of the methodology to respond to any

comments with any level or burden of technical thoroughness. Thus, the P81 SDT believes that FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 should remain within the scope of P81 for purposes of comment and ballot.

C. Suggested additions to the initial list

Comment

NPCC suggests adding FAC-003-1 R3, FAC-003-1 R4, CIP-005-3 R4, and CIP-007-3 R8.

Response

While the P81 SDT believes there appears to be merit in considering the FAC-003 and CIP requirements suggested by NPCC, these requirements were discussed in the collaborative process and it was generally agreed that these requirements need additional technical review prior to any consideration of retirement. Thus, these requirements will be considered in a subsequent phase of the P81 project.

Comment

NPCC and SRC suggest adding IRO-014-2 R2 and it sub-requirements. According to NPCC, these requirements are administrative requirements only and do not enhance reliability, while SRC states that these requirements satisfy Criterion B1 and Criterion B5.

Response

While IRO-014-2 R2 seems like a valid candidate for P81, it is not a FERC-approved Reliability Standard. At this time, it has been adopted by the NERC Board of Trustees and has yet to be filed with FERC for approval. As the P81 project matures or a more formalized approach to P81 is adopted by NERC in its Rules of Procedures or processes, the consideration of Reliability Standards not yet approved may be practical. However, at this time, the scope of the P81 project remains FERC-approved Reliability Standards. The exception to this is if a FERC-approved requirement being proposed for retirement is duplicated in a standard that has only been adopted by the NERC Board of Trustees. Thus, at this time, IRO-014-2 R2 is not ripe for consideration in P81.

Comment

ACES Power Marketing Standards Collaborators suggests adding FAC-010-2.1 R5 and FAC-011-2 R5 in the initial phase for the following reasons:

"FAC-010-2.1 R5 is an administrative requirement for the Planning Authority to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The PC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments. This requirement meets Criteria B.1 and B.9.(7) FAC-011-2 R5 is an administrative requirement for the Reliability Coordinator to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The RC is already required to distribute its methodology in R4."

Response

ACES Power Marketing Standards Collaborators' position is similar to the reasons that FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 were included in the draft SAR as satisfying the criteria and appropriate for retirement. Further, the language in all of these Reliability Standard requirements is very similar. Thus, the P81 SDT has added FAC-010-2.1 R5 and FAC-011-2 R5 to the initial phase of P81.

Comment

ACES Power Marketing Standards Collaborators suggests that IRO-005-3 R11 is redundant with MOD-028-1 R6.1, MOD-029-1a R3, and MOD-030-2 R2.4 and that the MOD standards already require the Transmission Service Provider to consider IROLs and SOLs when determining Available Transfer Capability/Available Flowgate Capability and Total Transfer Capability. Specifically, IRO-005-3 R11 reads:

"The Transmission Service Provider shall respect SOLs and IROLs in accordance with filed tariffs and regional Total Transfer Calculation and Available Transfer Calculation processes."

Response

It appears that while IRO-005-3 R11 may be redundant for the reasons stated by ACES Power Marketing Standards Collaborators; however, this requirement has been retired in IRO-005-4, which was approved by the Board of Trustees and is pending a filing at FERC. Thus, recognizing that that Project 2006-06 Reliability Coordination has already received many of the necessary approvals to retire IRO-005-3 R11, it does not seem to serve regulatory efficiency to include IRO-005-3 R11 in the P81 project as well. Thus, the P81 SDT did not add IRO-005-3 R11 to the initial phase of P81.

Comment

ACES Power Marketing Standards Collaborators suggests COM-001-1.1 should be retired because English is the dominant language used.

Response

To retire such a requirement would possibly need coordination with the Canadian authorities in French speaking provinces and those in areas of the United States were Spanish is a first language. Such coordination would seem to complicate the retirement of COM-001-1.1, and, thus, the P81 SDT believes it is more appropriately considered in a subsequent phase.

Comment

With regard to VAR-001-2 R5, ACES Power Marketing Standards Collaborators states that it:

". . . is redundant with FERC's pro forma tariff and was originally included in the NERC policies to align them with said tariff. The requirement compels the PSE and LSE to arrange for reactive resources to satisfy the reactive requirements of the Transmission Service

Provider. PSEs and LSEs cannot purchase transmission service without purchasing reactive service or demonstrating to the transmission provider that they have arranged for reactive resources. From a practical perspective, this means they always purchase reactive service from the Transmission Provider. Furthermore, it is the Transmission Operator that actually ensures reactive resources are dispatched per VAR-001-2 R2."

Response

The P81 SDT notes that when approving VAR-001, in Order No. 693 at Paragraph 1858,[5] the Commission recognized:

". . . that all transmission customers of public utilities are required to purchase Ancillary Service No. 2 under the OATT or self-supply, but the OATT does not require them to provide information to transmission operators needed to accurately study reactive power needs. The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities."

ACES Power Marketing Standards Collaborators states VAR-001-2 R5 appears to be redundant with Ancillary Service No. 2 under the OATT. Moreover, VAR-001-2 R5 is very limited to this OATT obligation and regional process, and, therefore, does not speak to the Commission's concern related to providing information to Transmission Operators for accurate reactive power studies. Therefore, it appears that VAR-001-2 R5 satisfies the P81 criteria by doing little to protect BES reliability and being redundant with the OATT. Thus, the P81 SDT has added VAR-001-2 R5 to the initial phase of P81.

Comment

ACES Power Marketing Standards Collaborators also suggests adding BAL-002 R1, BAL-002 R3, BAL-005-0.1b R1 and its sub-requirements, INT-004-2 R1, and TOP-005-2a R3.

Response

The P81 SDT notes that during the collaborative process the linkage between the BAL and INT standards was discussed and there seems to be merit considering whether some BAL and INT standards could be combined. The Trade Associations, among others, suggested this be conducted in a subsequent phase of P81. Given the complexity related to the linkage between the BAL and INT standards, along with TOP-005-2a R3, the P81 SDT believes that additional review should be conducted in a subsequent phase of P81 prior to retiring the suggested BAL and INT standards.

Comment

[5] VAR-001-2 was approved via a Letter Order issued on January 10, 2011.

ACES Power Marketing Standards Collaborators also suggests including PRC-011-0 R2, PRC-015-0 R3, PRC-016-0.1 R3, PRC-017-0.1 R2, PRC-021-0.1 R2, PRC-023-1 R2, and PRC-023-2 R3. American Electric Power suggests the following additions: PRC-021-1 R2; PRC-018-1 R5; PRC-016-0.1 R3; PRC-015-0 R3; PRC-011-0 R2; PRC-007-0 R3; CIP-006 R1.5; CIP-004-3 R4; CIP-007 R5.1.1; CIP-007 R5.1.3; CIP-007 R6.3; CIP-007 R6.4; CIP-003-3, CIP-003-4 R1; CIP-003-3, CIP-003-4 R1.2; CIP-003-3, CIP-003-4 R1.3; CIP-003-3, CIP-003-4 R2.4; CIP-003-3, CIP-003-4 R3. Tampa Electric recommends that the P81 SDT ensure that the CIP requirements proposed for removal via P81 are also removed from v5 of the NERC CIP standards. Tampa Electric also supports the consideration of the following for NERC CIP standards: (1) Removal of data collection requirements (CIP-005-3a,-4a R5.3, CIP-006-3c,-4c R7 and R8.3, CIP-007-3,-4 R5.1.2, R6.4and R7.3, CIP-008-3,-4 R2); and (2) Removal of annual review requirements (CIP-002-3,-4 R4, CIP-003-3,-4 R1.3, R4.3, R5.1.2, and R5.3, CIP-006-3c,-4c R1.8, CIP-007-3,-4 R9, and CIP-009-3,-4 R1).

Response

There was much discussion around the PRC and CIP standards during the collaborative process. There are several issues that impact the retirement of these requirements including not creating a reporting gap by retiring PRC standards and the coordination of CIP standards with the Version 5 SDT. Given these complications, the P81 SDT believes it is best to consider these CIP and PRC Standards as part of a subsequent phase of the P81 project. To address Tampa Electric's other concern, the P81 SDT has been coordinating its activities with the CIP Version 5 SDT, and will continue to do so, so that the agreed upon retirements do not reemerge in CIP Version 5.

Comment

Occidental Power Services, Inc. requests the removal of the PSE function from the applicable sections of the following: INT-001-3 R1, INT-004-2 R2, IRO-001-1.1 R3, IRO-001-1.1 R8, IRO-005-3 R10, TOP-005-2 R3, and VAR-001 R5. ACES Power Marketing Standards Collaborators also suggests removing PSE and LSE the applicable sections of IRO-005-3 R10.

Response

The removal of applicable from the requirements is an interesting suggestion that would take some more technical review and modification of the requirements. Thus, the P81 SDT believes this suggestion is more appropriate for consideration in a subsequent phase of P81.

Comment

Georgia Transmission Corporation suggests the following additions: MOD-016-1.1 R1, MOD-016-1.1 R1.1, MOD-016-1.1 R3, MOD-017-0.1 R1, MOD-017-0.1 R1.1, MOD-017-0.1 R1.2, MOD-017-0.1 R1.3, MOD-017-0.1 R1.4, MOD-018-0 R1, MOD-018-0 R1.2, MOD-018-0 R1.3, MOD-018-0 R2, MOD-019-0.1 R1, MOD-020-0 R1, MOD-021-1 R1, MOD-021-1 R2, MOD-021-1 R3, PRC-005-1b R2, PRC-005-1b R2.1, PRC-005-1b R2.2, PRC-006-1 R7, PRC-006-1 R8, PRC-006-1 R14, PRC-007-0 R2, PRC-007-0 R3, PRC-011-0 R2, PRC-015-0 R3, PRC-017-0 R2, PRC-018-1 R5, PRC-021-1 R2, PRC-023-1 R3.3, and TOP-001-1a R4.

Response

Georgia Transmission Corporation points out many of the same requirements that the trade associations suggest for subsequent phases of the P81 project. As mentioned above, for example, we are deferring the consideration of MOD-004-1 to a subsequent phase so it may be considered in the context of other MOD Standards. The P81 SDT believes it is more appropriate to consider Georgia Transmission Corporation's suggestions in a subsequent phase.

Comment

South Carolina Electric and Gas asked if the measures associated with requirements being proposed for retirement would be modified or removed as well.

Response

The relevant measures and other associated elements will be marked as retired in the standard. These will be identified in the redlines of the standards that will be posted with the requirements during the next comment period.

Comment

ERCOT states that the justification statement for BAL-005-0.1b R2 could benefit from additional clarification regarding how it is redundant with BAL-001 R1 and R2 and the justification for EOP-009-2 R2 should also be enhanced.

Response

The P81 SDT notes that additional clarification for BAL-005-0.1b R2, EOP-009-0 R2 and other requirements will be included in the technical white paper being developed by the P81 SDT.

In summary, of the initial list in the draft SAR, MOD-004-1, VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2 have been deferred to a subsequent phase. Of the suggested additions, it appears that only VAR-001-2 R5, FAC-010-2.1 R5 and FAC-011-2 R5 satisfy the P81 criteria without significant technical review, and, thus, are appropriate to be added to the final SAR for the initial phase. As a general note, any requirements suggested for the initial phase, but not adopted, shall be considered by the P81 SDT in a subsequent phase of the project, and, therefore, the entities do not need to resubmit the requirements.

Organization	Yes or No	Question 2 Comment
Northeast Power Coordinating Council	No	From page 25 of the SAR, "Since PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 provides little protection to the BES and better handled under event analysis and lessons learned papers, it should be removed." is not valid due to that fact that as of this posting the Event Analysis Program (EAP) has not become part of the RoP and is therefore a voluntary program. The requirements that are covered by these standards are mandatory cannot be replaced by a voluntary program. Refer to the following:Additionally, the EAP process is an after-the-fact Analysis of an event or events. These standard requirements (PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2) address different needs which can be determined only if such an event occurs. For example, from PRC-008-0--"R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance." This requirement addresses the need to have an equipment maintenance and testing program in place prior to an event. Discovering that an entity did not have this as a result of an event analysis would, in this case, be after the damage is done and would not serve reliability. Analyzing why the UFSL program did not operate properly would come under the purview of the EAP but that is different from the Standard's intent. PRC-008-0--"R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days)." If the EAP was relied upon to meet this requirement the receipt or confirmation of this program would only occur after an event. PRC-009-0--"R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall

Organization	Yes or No	Question 2 Comment
		analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:R1.1 A description of the event including initiating conditions.R1.2 A review of the UFLS set points and tripping times.R1.3 A simulation of the event.R1.4 A summary of the findings."Although this Standard appears that it could be covered under EAP, it is a highly detailed technical study and needs to be carried out on its own accord. Event Analysis will focus primarily what caused the event that triggered the UFLS program but not necessarily the program itself. Because of the importance of the UFLS program to the reliability of the system, its performance should not be analyzed only on a voluntary basis and not only by those entities that actually shed load as a result of the event, but against the whole regional program.PRC-009-0--"R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event."This is administrative, refer to the response for R1 preceding. PRC-010-0--"R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days)." This should not triggered only after an event, see preceding response for R1 preceding. PRC-022-1--"R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request."This is the same situation as for the UFLS program. Refer to the responses preceding. IRO-014-2 --The following requirements in Standard IRO-014-2 are administrative requirements only and do not enhance reliability, and should be considered for removal in the Initial

Organization	Yes or No	Question 2 Comment
		Phase. "R2. Each Reliability Coordinator shall maintain its Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 as follows: [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]2.1. Review and update annually with no more that 15 months between reviews. 2.2. Obtain written agreement from all of the Reliability Coordinators required to take the indicated action(s) for each update.2.3. Distribute to all Reliability Coordinators that are required to take the indicated action(s) within 30 days of an update."FAC-003-1 Requirements R3, and R4 (shown below) and their sub-requirements are administrative (reporting) requirements only and do not enhance reliability, and should be considered for removal in the Initial Phase. R3. The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.R4. The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions taken by the RRO as a result of any of the reported outages.In addition, as shown below, CIP-005-3 R4 and CIP-007-3 R8 are essentially the same. Suggest to eliminate CIP-005-3 R4 and include assessment of access points in CIP-007-3 R8.CIP-005-3 R4:"R4. Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following: R4.1. A document identifying the vulnerability assessment process; R4.2. A review to verify that only ports and services required for operations at these access points are enabled; R4.3. The discovery of all access points to the Electronic Security Perimeter; R4.4. A review of controls for default accounts, passwords, and network management community strings; R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan." CIP-007-3 R8:"R8. Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the

Organization	Yes or No	Question 2 Comment
		following: R8.1 A document identifying the vulnerability assessment process; R8.2 A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled; R8.3 A review of controls for default accounts; and, R8.4 Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan."
Southwest Power Pool Regional Entity	No	SPP RE does not agree that PRC-008 R1 and R2 should be retired or that they provide "little protection to the BES and [are] better handled under event analysis and lessons learned papers". UFLS equipment maintenance and testing programs ARE important to BES reliability, in a preventative mode, and are NOT covered under the Event Analysis process. Preventative maintenance is very important to reliability; without it, events are more likely. Industry should not wait for an event to happen to collect information and consider maintenance and testing. UFLS is the last line of "defense in depth protection of the BES" (Criteria C6). SPP RE's comment follows the discussion around removing PRC-005 and its relationship to BES reliability.SPP RE does not agree that CIP-007-3 R7.3 should be retired. R7.3 requires the Responsible Entity to maintain records of how data storage media was erased or destroyed prior to disposal or redeployment of the Cyber Asset (which could be simply the media previously removed from the Cyber Asset). In the absence of such records, the Responsible Entity cannot demonstrate compliance with CIP-007-3 R7.1 and CIP-007-3 R7.2, rendering those requirements not auditable. Elimination of this requirement could also result in a loss of visibility of Cyber Assets that have been disposed of or redeployed, also hampering the ability of the Responsible Entity to demonstrate compliance and the Compliance Enforcement Authority to audit compliance with the remaining requirements.
Bonneville Power Administration	No	BPA does not support the proposed retirement of TOP-001-1a R3. BPA does not agree that TOP-001-1a R3 is redundant with IRO-001-1a R8 because IRO-001-1a R8 only addresses RC directives, whereas TOP-001-1a R3 addresses both RC directives and TOP directives. BPA believes that retiring TOP-001-1a R3 before TOP-001-2 R1 is

Organization	Yes or No	Question 2 Comment
		effective would create a gap because no requirement would address TOP directives. BPA supports the additional proposed retirements and thanks the drafting team for their efforts.
ACES Power Marketing Standards Collaborators	No	(1) We believe there are other requirements that easily meet the criteria. (2) VAR-001-2 R5 is redundant with FERC's pro forma tariff and was originally included in the NERC policies to align them with said tariff. The requirement compels the PSE and LSE to arrange for reactive resources to satisfy the reactive requirements of the Transmission Service Provider. PSEs and LSEs cannot purchase transmission service without purchasing reactive service or demonstrating to the transmission provider that they have arranged for reactive resources. From a practical perspective, this means they always purchase reactive service from the Transmission Provider. Furthermore, it is the Transmission Operator that actually ensures reactive resources are dispatched per VAR-001-2 R2. Thus, VAR-001-2 R5 satisfies criteria B.1, B.6, B.7, and B.9.(3) BAL-002 R1 and R3 are redundant. R1 compels the BA to have access to and operate Contingency Reserve to respond to disturbances. R3 requires the BA to activate sufficient Contingency Reserve to comply with DCS. We suggest removing R1 because it is redundant (Criterion B.7). This applies to both versions 0 and 1 of the standard.(4) BAL-005-0.1b R1 and its sub-requirements are not necessary. All generation, transmission and load is currently contained within the metered boundaries of a BA. It is impossible to add new generation, transmission and load and not be within the metered boundaries of a BA. To do so, would require the equipment owner to carve out an area from the BA. For example, if a TO added a new transmission line, it would have to put a meter on both ends to carve it out of any BA footprint. In the process, they, in effect, create a new BA. The only way these requirements can't be met would be if BAs started removing metering equipment en masse. Given removing metering equipment has significant financial consequences due to inaccurate energy accounting; it is not going to happen. Thus, it meets Criterion B.9. Furthermore, TOs are already required to identify metering requirements in FAC-001-0 R2.1.6 as part of its facility connection requirements. It also meets Criterion B.7.(5) COM-001-1.1 is unnecessary and the audit of it has

Organization	Yes or No	Question 2 Comment
		largely become a demonstration that it is an administrative requirement. English is the primary language across the vast majority of the Interconnections under NERC's purview and it is the primary language in all of the areas under FERC's jurisdiction. For the few companies in areas where English is not predominant, those companies will be unable to meet other requirements if they use a different language to speak with companies from predominantly speaking English languages. Furthermore, audits have regulated this to predominantly an administrative requirement. The auditors largely look for statement that the English language is required despite the fact that all evidence has been provided in English, observations of control center conversations have shown English is used, and the audit has been conducted in English. If there is a need for this requirement, it should be relegated to a regional requirement for those regions that include areas that do not speak predominantly English. Thus, this requirement meets Criteria B.1 and B.9.(6) FAC-010-2.1 R5 is an administrative requirement for the Planning Authority to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The PC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments. This requirement meets Criteria B.1 and B.9.(7) FAC-011-2 R5 is an administrative requirement for the Reliability Coordinator to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The RC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments when they receive the methodology. This requirement meets criteria B.1 and B.9.(8) INT-004-2 R1 has nothing to do with reliability and should be included in the list of retirements. Failing to reload an Interchange Transaction that was curtailed for a reliability event has no reliability impact. It is a remnant from the NERC Policies that was added at the request of market participants because once transactions were cut, reliability entities did not always allow the transaction to resume once the reliability issue had been addressed. This is strictly a commercial issue. Thus, this requirement meets Criterion B.9.(9)

Organization	Yes or No	Question 2 Comment
		IRO-005-3 R10 should be modified to reflect the functional model. In cases where there are differences in derived limits, PSEs and LSE cannot operate to the most limiting parameters. They are not in a position to even have information on the parameters such as facility ratings. Rather, their role is to follow directives. Thus, inclusion of PSE and LSE in the requirement does not support reliability. Thus, this requirement meets Criterion B.9. (10) IRO-005-3 R11 is redundant with MOD-028-1 R6.1, MOD-029-1a R3, and MOD-030-2 R2.4. The MOD standards already require the TSP to consider IROLs and SOLs when determining Available Transfer Capability/Available Flowgate Capability and Total Transfer Capability. This requirement meets Criterion B.7. (11) PRC-011-0 R2 should be retired. A requirement is not needed to compel the TO and DP to provide data on its UVLS equipment maintenance program to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(12) PRC-015-0 R3 should be retired. A requirement is not needed to compel the TO, GO and DP to provide data on their Special Protection Systems (SPS) to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(13) PRC-016-0.1 R3 should be retired. A requirement is not needed to compel the TO, GO and DP to provide data on their SPS Misoperations analyses and corrective action plans to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(14) PRC-017-0.1 R2 should be retired. A requirement is not needed to compel the TO, GO and DP to provide documentation of the SPS maintenance and testing program to the Regional Entity. The Regional Entities CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(15) PRC-

Organization	Yes or No	Question 2 Comment
		021-0.1 R2 should be retired. A requirement is not needed to compel the TO and DP to provide UVLS program data to the Regional Entity. The Regional Entities CMEP and NERC's Rules of Procedure compel the TO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(16) PRC-023-1 R2 and PRC-023-2 R3 are redundant with FAC-008-1 R1.2.1 and FAC-008-3 Part 2.4.1. FAC-008-1 R1.2.1 and FAC-008-3 Part 2.4.1 already require the GO and TO to consider relay protective devices when determining facility ratings. The DP cannot limit the Facility Rating because a DP does not have Transmission Facilities. They only have relays that impact Facility Ratings that must ultimately be considered by the TO. This requirement meets Criterion B.7(17) TOP-005-2a R3 is redundant with the INT standards and should be retired. In the NERC Functional Model, the only role for the PSE is to facilitate Arranged Interchange. The INT standards already govern Arranged Interchange and contain the necessary information that the PSE must provide. Furthermore, Project 2007-03 Real-Time Operations has proposed retirement of this requirement as it is redundant with NAESB e-Tag specifications. Beyond the E-tag data there is no additional information that a PSE or LSE could provide for the BA or TOP to conduct operational assessments. This requirement meets Criteria B.6, B.7 and B.9.(18) PRC-006-1 R7 should be retired. Failure by a Planning Coordinator to provide data to another Planning Coordinator within 30 days is not a reliability issue because Planning Assessments have long time lines to complete the studies. Furthermore, any failure to provide data within 30 calendar days is most likely a simple oversight. If a Planning Coordinator refuses to provide data, the requesting Planning Coordinator may get involved and which will compel them to provide the data. This can be done without the need for this requirement. This requirement meets criterion B.4.
Western Electricity Coordinating Council	No	WECC supports the majority of the Standards Requirements identified, but notes concerns with the following. WECC recommends eliminating CIP-003 R1 in its entirety.WECC disagrees with the inclustion of CIP-007, R7.3. This requirement is necessary for entity's to demonstrate compliance with the other sub-requirements of CIP 007 R7. However, this requirement could be moved to a Measure or RSAW to

Organization	Yes or No	Question 2 Comment
		demonstrate compliance with the other sub-requirements of CIP-007, R7.WECC disagrees with the includsion of IRO-016-1, R2. Required documentation of the RC's actions to remedy an event is necessary for quality and efficient root cause analysis, including insight into the RC's wide view of actions during an event or disagreement. The language in the SAR statement for IRO-016-1 R2 points to this information being monitored through Spot Checks or other compliance monitoring methods. If this standard is removed yet the information is to be included in future compliance monitoring there must be some sort of methodology that requires the entity to retain the associated data to be kept for the duration of the required cycle for monitoring (i.e. audit cycle if monitored through audits). It is important that entities document the actions taken that analyze the effect on the system as well as the BES for either an even or/and for the disagreement on the problem. Therefore, it is important that this information is part of the overall compliance monitoring program.MOD-004 is not redundant to TOP-002 even though the CBM itself may be a tariff issue and rarely used. The reliability piece is that if the CBM is used by a TSP then the details of it must be available for use in system studies. Without the awareness of a transmission holdback for CBM when it exists, a network study could be run and show no issues but if at some time the CBM were implemented an overload could result. This might not always be the case but unless the CBM parameters are known and modeled it could impact reliability.WECC disagrees with the recommendations with PRC-008-0 R1 and PRC-008-0 R2. Unless these standards are being superseded, WECC does not agree that they provide "little protection to the BES." They are not administrative in nature like the other standards in this group. They insure that maintenance and testing program is established and implemented for an entity's UFLS protection systems. Without these standards, there is reduced assurance that UFLS protection systems will operate correctly when called upon for an under-frequency event. UFLS has a vital role in its effectiveness for preserving system stability and elimination of these standards may reduce its effectiveness. This standard is about making sure the equipment is maintained not about collecting data. If and when PRC-005-2 is adopted, and if it were to include the UFLS devices, then this standard should be

Organization	Yes or No	Question 2 Comment
		considered for removal.WECC believes the statements associated with TOP-001-1a, R3 are incorrect. Removing TOP-001-1a would result in no NERC requirement for parties to follow TOP directives. The current TOP-001-1a R3 requires BOTH TOP and RC directives to be followed. The proposed IRO-001-3 R2 requires ONLY RC directives to be followed. In addition, the SAR statement is incorrect. TOP-001-1a R3 applies to directives issued by the TOP (and also the RC). IRO-001-1a applies only to directives from the RC. If the intent, as they state, is to replace TOP-001-1a R3 with IRO-001-3, that leaves a void for an entity to comply with a directive from the TOP. Only the part about following an RC directive is redundant. Requirement should be modified to eliminate the redundancy, but not retired. WECC disagrees witht he inclusion of CIP-001, R4. An entity has many enforcement agencies to contact without the FBI listed in the operating instructions they could easily be overlooked. This Requirement has encouraged entities to establish a current communication line with the FBI. In fact, several other larger entities are members of InfraGardÂ®, which is a partnership between the FBI and the private sector. Retiring R4 will remove the incentive of having a working relationship with the FBI, especially among the smaller entities. Retiring R4 may effectively delay or prevent the FBI from rapidly locating those responsible for sabotage. The requirement is not “needlessly burdensome”, which is a criteria for deletion.WECC believes the requirements VAR-002-WECC-1, R2, and VAR-502-WECC-1, R2, are probably the best way of demonstrating compliance with the accociated R1 requirments. The two VAR R2 requirements do not say the entity has to submit the information to WECC (Regional Entity), only that it shall have the documentation to prove exclusion for the sub requirements in R1. We’ve had cases where entities don’t meet the 98% availability and if the entity was claiming exclusion time, WECC would want to review the documentation that proves the exclusion. It is in the entity’s best interest to keep exclusion documentation in case its units don’t make the 98%, but this is beter suited for a Measure or RSAW.
Independent Electricity System Operator	No	(1) We generally agree that most of the identified standards/requirements would meet the proposed criteria. However, as indicated under Q1, we believe that the “annual review” criterion is too broad which could result in retiring some

Organization	Yes or No	Question 2 Comment
		requirements that are still needed for reliability. In addition, the acid test for retirement a requirement is when the standard drafting team reviews the overall reliability impact of removing a particular requirement from a standard, and how it may affect other related standards. In brief, it is premature to pass on this judgment at the SAR stage. We urge the SAR proponent to simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired. And, in order to meet the requirements for regulatory approval, we suggest the SDT to provide strong technical basis to justify each retirement.
American Electric Power	No	AEP does not disagree with a majority of the requirements proposed by the drafting team, though we recommend the team reconsider the inclusion of CIP-003 R3 and associated sub-requirements. AEP recommends instead that CIP-003 R1 be removed in which case CIP-003 R3 (and CIP-003 R2.4) can also be removed. However, if the drafting team does not agree with this recommendation, CIP-003 R3 must be retained in order for entities to take targeted exception(s) where applicable (for example, in circumstances where an entity's program is more stringent than the CIP requirements).AEP would like the team to consider the following additional Reliability Standard requirements as candidates for retirement on this initial, or subsequent, request for comment. Standard: PRC-021-1Requirement: R2Requirement Text: Each Transmission Operator and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.Criterion: B4,9Standard: PRC-018-1Requirement: R5Requirement Text: The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.Criterion: B2Standard: PRC-016-0.1Requirement: R3Requirement Text: The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).Criterion: B4Standard: PRC-015-0Requirement:

Organization	Yes or No	Question 2 Comment
		R3Requirement Text: The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of Studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).Criterion: B4Standard: PRC-011-0Requirement: R2Requirement Text: The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days).Criterion: B4Standard: PRC-007-0Requirement: R3Requirement Text: The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days).Criterion: B4Standard: CIP-006Requirement: R1.5Requirement Text: Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.Criterion: B7Standard: CIP-007Requirement: R5.1.1Requirement Text: The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.Criterion: B7Standard: CIP-007Requirement: R5.1.3Requirement Text: The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.Criterion: B7Standard: CIP-007Requirement: R6.3Requirement Text: The Responsible Entity shall maintain logs of system events related to cyber security, where technically Feasible, to support incident response as required in Standard CIP-008-3.Criterion: B7Standard: CIP-007Requirement: R6.4Requirement Text: The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.Criterion: B1, B3Standard: CIP-003-3, CIP-003-4Requirement: R1Requirement Text: Cyber Security Policy - The Responsible Entity shall document and implement a cyber security policy that represents

Organization	Yes or No	Question 2 Comment
		management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:Criterion: B1, B3, B7, B9Standard: CIP-003-3, CIP-003-4Requirement: R1.2Requirement Text: The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. Criterion: B1, B3, B7, B9Standard: CIP-003-3, CIP-003-4Requirement: R1.3Requirement Text: Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2. Criterion: B5Standard: CIP-003-3, CIP-003-4Requirement: R2.4Requirement Text: The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy. Criterion: B7Comment: Although AEP does not necessarily agree with removal of this requirement (see R3 comment below), R2.4 is redundant with R3.3 (which is being removed) and should probably be removed along with R3.Standard: CIP-003-3, CIP-003-4Requirement: R3 (R3.1, R3.2, R3.3)Requirement Text: Exceptions - Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). Criterion: Comment: If R1 is not removed, R3 (or some exception process) is necessary. For example, if the Cyber Security Policy goes above and beyond the standards, then an exception may be needed even though the standards are met.
Public Service Enterprise Group	No	For these requirements, KEEP:CIP-001-2a R4. If the entity owns or operates a BES asset, there is a clear reliability benefit to have appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to these Law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response. Thus we feel that this requirement should be kept within the standards.CIP-003-3 R3. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. It's removal may have a negative impact on the industry. CIP-003-4 R3. The exceptions language in R3, though

Organization	Yes or No	Question 2 Comment
		rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. It's removal may have a negative impact on the industry. TOP-005-2a R1. "TOP-003-2 requires operating entities such as GOs and TOs to provide operating data to BAs ands TOPs. In TOP-005-2a, R2 and R3 requires BAs and TOPs to exchange this data with other BAs and TOPs . R1 requires BA and TOP recipients of such data to execute a confidentiality agreement so that its confidentiality is protected. This requirement ultimately protects the confidentiality of data provided by entities under TOP-003-2.For these requirements, KEEP BUT MODIFY:FAC-002-1 R2. We believe the three year limitation on documentation sets a limit; otherwise six years may be required (the period between audits. We do suggest removing the language " and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days)." because we see no reliability benefit.For these rerquirements, KEEP UNTIL REPLACED:EOP-004-1 R1. NERC's Event Analysis Process was approved by NERC's BOT on February 9, 2012. This process has already been adopted as RFC's process under EOP-004-1, R1. Draft standard EOP-004-2 will replace Regional reporting requirements in R1 with consistent NERC-wide requirements; however, while the draft does not presently require the use of the NERC Event Analysis Process, that process is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. Keep until these NERC ROP changes are approved by FERC and become effective.PRC-008-0 R1. This is required for reliability. Such a testing program has been incorporated into draft PRC-005-2 When this is adopted, PRC-008-0 can be retired.PRC-009-0 R1. The NERC Event Analysis Process is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. Keep until these NERC ROP changes are approved by FERC and become effective.PRC-009-0 R1.1. See R1 above.PRC-009-0 R1.2. See R1 above.PRC-009-0 R1.3. See R1 above.PRC-009-0 R1.4. See R1 above.
Essential Power, LLC	No	CIP-001-2a, R4. This requirement should be removed from the Paragraph 81 project. If an entity owns or operates a BES asset, there is a clear reliability benefit to have

Organization	Yes or No	Question 2 Comment
		appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to these law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response. Thus we feel that this requirement should be kept within the standards.CIP-003-3, R3. This requirement should be removed from the Paragraph 81 project. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform to its cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. Its removal may have a negative impact on the industry.CIP-003-4, R3. This requirement should be removed from the Paragraph 81 project. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform to its cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. Its removal may have a negative impact on the industry.EOP-004-1, R1. This requirement should be removed from Phase 1 of the Paragraph 81 project, until replaced by EOP-004-2. NERC's Event Analysis Process was approved by NERC's BOT on February 9, 2012. This process has already been adopted as RFC's process under EOP-004-1, R1. Draft standard EOP-004-2 will replace Regional reporting requirements in R1 with consistent NERC-wide requirements; however, while the draft does not presently require the use of the NERC Event Analysis Process, which is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. This requirement should be kept until these NERC ROP changes are approved by FERC.FAC-002-1, R2. This requirement should be removed from the Paragraph 81 project, and modified instead. We believe the three year limitation on documentation sets a limit; otherwise six years may be required (the period between audits). We do suggest removing the language “and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days)." because we see no reliability benefit to this element of the requirement.
Occidental Power Services,	No	OPSI recommends the following additions for Phase 1 implementation: 1. INT-001-3, R1. The Load Serving, Purchasing-Selling Entity shall ensure that Arranged

Organization	Yes or No	Question 2 Comment
Inc.		Interchange is submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.Criteria: B6, B9Statement: This requirement is at best a business practice of markets (protocol). These schedules can be rejected if not correctly submitted, can be cut if not executed correctly, and the PSE can be penalized if there are offenses.Recommendation: Remove PSE from R1 and from the Applicability section.2. INT-004-2, R2. The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:o R2.1 The average energy profile in an hour is greater than 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than Â±10%o R2.2 The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than Â±25 megawatt-hourso R2.3 A Reliability coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons. Criteria: B6,B9Statement: This requirement is at best a business practice of markets (protocol). These schedules can be rejected if not correctly submitted, can be cut if not executed correctly, and the PSE can be penalized if there are offenses.Recommendation: Remove PSE from R2 and from the Applicability section.3. IRO-001-1.1, R3 and R8.R3. The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing- Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes.R8. Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the

Organization	Yes or No	Question 2 Comment
		Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.Criteria: B9Statement: PSEs do not generally receive Reliability Directives from RCsRecommendation: Remove PSE from R3 and R8 and from the Applicability section.4. IRO-005-3, R10. In instances where there is a difference in derived limits, the Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall always operate the Bulk Electric System to the most limiting parameter.Criteria: B9Statement: PSEs do not generally derive limits for the transmission of power over the BES.Recommendation: Remove PSE from R10 and from the Applicability section.5. TOP-005-2, R3. Each Purchasing-Selling Entity shall provide information as requested by its Host Balancing Authorities and Transmission Operators to enable them to conduct operational reliability assessments and coordinate reliable operations.Criteria: B6,B9Statement: PSEs have to supply this information as a requirement for participating in market functions.Recommendation: Remove PSE from R3 and from the Applicability section.6. VAR-001, R5. Each Purchasing-Selling Entity shall arrange for (self-provide or purchase) reactive resources to satisfy its reactive requirements identified by its Transmission Service Provider.Criteria: B6,B9Statement: This is a requirement to participate in competitive markets (generally, it is included in the transmission rate) or is required by tariffs in non-competitive markets. The PSE has no option but to purchase the reactive power in order to make the transaction.Recommendation: Remove PSE from R5 and from the Applicability section.
Georgia Transmission Corporation	No	GTC agrees that the suggested list easily satisfies the criteria in the draft SAR, but GTC also believes this is an incomplete list for Phase I. GTC also believes the following Reliability Standard requirements easily satisfy the criteria listed in the draft SAR and recommends reconsidering and adding to the list in the initial Phase I.MOD-016-1.1;R1:The Planning Authority and Regional Reliability Organization shall have

Organization	Yes or No	Question 2 Comment
		documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses. [Meets Criteria A, B1, B2, B3, B9]MOD-016-1.1 R1.1 The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values. Meets Criteria A, B1, B3, B4, B9MOD-016-1.1 R3 The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area. Meets Criteria A, B1, B3, B9MOD-016-1.1 R3.1 The Planning Authority shall make this distribution within 30 calendar days of approval. Meets Criteria A, B1, B3, B9MOD-017-0.1 R1 The Load-Serving Entity, Planning Authority and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R1. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.1 Integrated hourly demands in megawatts (MW) for the prior year. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.2 Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.3 Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.4 Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested. Meets Criteria A, B1, B4, B9MOD-018-0 R1 The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or

Organization	Yes or No	Question 2 Comment
		dispersed basis) shall: Meets Criteria A, B1, B3, B9MOD-018-0 R1.1 Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and Meets Criteria A, B1, B3, B9MOD-018-0 R1.2 Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load. Meets Criteria A, B1, B3, B9MOD-018-0 R1.3 Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1. Meets Criteria A, B1, B3, B9MOD-018-0 R2. The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days). Meets Criteria A, B1, B4, B9MOD-019-0.1 R1. The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-1_R 1. Meets Criteria A, B1, B4, B9MOD-020-0 R1. The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days. Meets Criteria A, B1, B4, B9MOD-021-1 R1. The Load-Serving Entity, Transmission Planner and Resource Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed. Meets Criteria A, B1, B3, B9MOD-021-1 R2. The Load-Serving Entity, Transmission Planner and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy

Organization	Yes or No	Question 2 Comment
		for Load in the data reporting procedures of Standard MOD-016-0_R1. Meets Criteria A, B1, B3, B9MOD-021-1 R3. The Load-Serving Entity, Transmission Planner and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B9PRC-005-1b R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include: Meets Criteria A, B1, B3, B9PRC-005-1b R2.1. Evidence Protection System devices were maintained and tested within the defined intervals. Meets Criteria A, B1, B3, B9PRC-005-1b R2.2. Date each Protection System device was last tested/maintained. Meets Criteria A, B1, B3, B9PRC-006-1 R7. Each Planning Coordinator shall provide its UFLS database containing data necessary to model its UFLS program to other Planning Coordinators within its Interconnection within 30 calendar days of a request. Meets Criteria A, B1, B4, B9PRC-006-1 R8. Each UFLS entity shall provide data to its Planning Coordinator(s) according to the format and schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. Meets Criteria A, B1, B4, B9PRC-006-1 R14. Each Planning Coordinator shall respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the following:14.1. UFLS program, including a schedule for implementation 14.2. UFLS design assessment 14.3. Format and schedule of UFLS data submittal Meets Criteria A, B1, B3, B9PRC-007-0 R2. The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a

Organization	Yes or No	Question 2 Comment
		UFLSprogram database. Meets Criteria A, B1, B4, B9PRC-007-0 R3. The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days). Meets Criteria A, B1, B3, B4, B9PRC-011-0 R2. The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B4, B9PRC-015-0 R3. The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days). Meets Criteria A, B1, B4, B9PRC-017-0 R2. The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B4, B9PRC-018-1 R5. The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years. Meets Criteria A, B1, B2, B3, B9PRC-021-1 R2. Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request. Meets Criteria A, B1, B4, B9PRC-023-1 R3.3. The Planning Coordinator shall provide a list of facilities to its Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within 30 days of the establishment of the initial list and within 30 days of any changes to the list. Meets Criteria A, B1, B4, B9TOP-001-1a R4. Each Distribution Provider and Load-Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory

Organization	Yes or No	Question 2 Comment
		requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions. Same requirement as R3 which made the Phase I list, only difference is applicability.
NERC Staff Technical Review	No	After further review, NERC Staff recommends that the SDT review the following standard requirements and consider moving them from Phase I to Phase II. If the SDT determines the following standard requirements still fall into Phase I, a more robust technical justification would be needed.(1) FAC-008-1 R2, R3, FAC-008-3 R4, R5 and FAC-013-2 R3: These requirements, combined with others, provide checks and balances on the Facility Rating Methodology and Transfer Capability methodology established by the responsible entities. This provides a reliability benefit by requiring the responsible entity to consider areas in which their methodology may not be sufficient to support reliable operation of the interconnected transmission system. There may be better ways of assuring that entities have sufficient methodologies and alternatives should be considered during Phase II. NERC Staff suggests that the SDT reconsider whether discussing the methodology (and not the numerical rating of a facility) has commercial or market related implications. With respect to FAC-013-2 R3, NERC Staff suggests that the SDT reconsider whether the requirement relates to "a back and forward on transfer capability" as noted in the draft SAR, as the requirement pertains only to the methodology for determining transfer capability.(2) PRC-008-0 R2: Maintenance and testing of underfrequency load shedding (UFLS) relays is necessary to assure reliable operation of a UFLS program and this requirement is included in PRC-005-2 as part of Project 2007-17, Protection System Maintenance and Testing. NERC Staff recommends that the language in R2 relating to implementing its UFLS equipment maintenance and testing program remain to avoid a reliability gap prior to the effective date of PRC-005-2. NERC Staff recognizes that the second part of R2 does meet the criteria in the SAR and recommends that the SDT consider revising the requirement in a future phase to remove the language that requires an entity to "provide UFLS maintenance and testing program results to

Organization	Yes or No	Question 2 Comment
		its Regional Reliability Organization and NERC on request (within 30 calendar days)." (3) TOP-001-1a R3: The technical justification states that this requirement is redundant with IRO-001-1a R8. NERC Staff notes that the requirement is only partially redundant until IRO-001-3 is approved by FERC and therefore, it is premature to consider it for Phase I; it should be considered for Phase II.(4) MOD-004-1: NERC Staff notes that there are a number of Commission directives associated with MOD-004-1 and the technical justification provided for the elimination of this standard should directly address these directives. If a solid technical justification cannot be made, NERC Staff suggests that the requirements should not be included in Phase I. In addition to the above, NERC Staff recommends that the SDT consider removing the following standard requirements from the scope of the P81 project:(1) PRC-008-0 R1: The requirement to have a maintenance and testing program for UFLS is necessary to assure reliable operation of a UFLS program and this requirement is included in PRC-005-2 as part of Project 2007-17, Protection System Maintenance and Testing. NERC Staff recommends retaining R1 to avoid a reliability gap prior to the effective date of PRC-005-2.(2) PRC-009-0 R1: Analysis to assess the performance of UFLS equipment and program effectiveness following system events provides a reliability benefit by identifying whether the UFLS program is effective and whether modifications are necessary. A requirement similar to R1 is included in FERC-approved standard PRC-006-1 and NERC Staff recommends retaining R1 to avoid a reliability gap prior to the effective date of PRC-006-1. If the SDT believes this requirement is not necessary, the justification for removing R1 should discuss Commission comments in Order No. 763 pertaining to Requirement R11 in PRC-006-1.(3) VAR-002-WECC-1 and VAR-501-WECC-1: NERC Staff notes that the regional standards should be removed from the scope of the P81 project because they must first be eliminated via the regional standards development process prior to being processed through the NERC standard development process.
MidAmerican Energy Company	No	FERC Order 706 clearly states that an exception forms alternative obligations for the responsible entity to meet the requirements; an exception is not an exemption from the requirements. We believe a Responsible Entity should still be allowed to have

Organization	Yes or No	Question 2 Comment
		exceptions to its cyber security policy. MidAmerican Energy Company agrees with the proposed removal of CIP-003-3 (CIP-003-4) R3, R3.1, R3.2, R3.3, as long as CIP-003-3 (CIP-003-4) R2.4 remains and allows for possible exceptions to a Responsible Entities' cyber security policy. R2.4 states "The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy." When removing requirements eligible for TFEs, revisions to the Rules of Procedure Appendix 4D - Procedures for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards will be necessary. For example, CIP-005-3, R2.6 should be deleted from the list of requirements with TFEs in the Scope section on page 1 if the requirement is removed as part of this process.
SPP Standards Review Group	Yes	From our review of the list we feel that this is again, a good starting point, but would hope that the drafting team could add or subtract requirements as needed as Phase 1 of the project develops.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade Associations).	Yes	The Trade Associations agree with the suggested list of Reliability Standard requirements contained in the SAR for the Initial Phase of P81.

Organization	Yes or No	Question 2 Comment
Salt River Project	Yes	Yes
SRC	Yes	o PRC-009-0 R1 - R2 are in the process of being retired by PRC-006-1 as such these requirements will eventually go away. o VAR-002-WECC-1 R2 - Regional standards/requirements for retirement should go through the regional standards process not the NERC continent wide process. o VAR-501-WECC-1 R2 - Regional standards/requirements for retirement should go through the regional standards process not the NERC continent wide process. o Consider adding IRO-014-2 R2 requirements: R2 Each Reliability Coordinator shall maintain its Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 as follows: [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]2.1. Review and update annually with no more that 15 months between reviews. 2.2. Obtain written agreement from all of the Reliability Coordinators required to take the indicated action(s) for each update.These meet criteria B1 and B5.
Georgia System Operations Corporation	Yes	Georgia System Operations agrees with the suggested list of Reliability Standard requirements contained in the SAR for the Initial Phase of P81.
seattle city light	Yes	Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Duke Energy	Yes	The initial phase of the P81 project should contain only requirements that can quickly gain industry and regulatory support and that there is adequate time to prepare a strong technical justification for. Duke Energy asks the P81 Standards Drafting Team to ensure these parameters are taken into consideration as the list is finalized, and move to a subsequent phase any requirements that could take additional time to develop a strong technical justification and consensus for.

Organization	Yes or No	Question 2 Comment
NV Energy	Yes	Our review of the rationale for each of the suggested requirements of the draft SAR supports the conclusion that these requirements should be subject to retirement.
Occidental Energy Ventures Corp.	Yes	OEVC believes that the phased approach proposed in the SAR is prudent and likely the most effective. Only the most obvious candidates for retirement or modification should be presented at this early date. If the industry moves too-far, too-fast, the result may be a blanket rejection of every proposal. Once FERC is comfortable that the industry is in-tune to their sense of risk - which includes public perception of their oversight effectiveness - we believe they will be prepared to deal with requirements that seem important on the surface, but whose contribution to reliability is illusory.
South Carolina Electric and Gas	Yes	Will the measures associated with requirements that are up for retirement be modified or removed?Eg. Removing R2 of a standard but not removing the text in M1 which refers to R2 of that same standard.
Ameren	Yes	We appreciate the excellent work done by the P81 Project team in developing the criteria and agree with the list of suggested standards/requirements that easily satisfy the criteria in this initial phase.
Electric Reliability Council of Texas, Inc.	Yes	ERCOT agrees with the ISO/RTO SCR comments. However, in addition to the SRC comments, ERCOT offers the following:ERCOT agrees that all the requirements included in the SAR warrant retirement based on the relevant criteria, as supported by the corresponding justification statements. ERCOT offers the following additional comments related to the justification statements for the SDT's consideration:BAL-005-0.1b R2 - The justification statement could benefit from additional clarification regarding the reason why this requirement is redundant, because it isn't readily apparent why this is redundant with BAL-001 R1 and R2. Maintaining CPS requires the use of regulation. Therefore, it is implicit that the relevant functional entities have regulation to comply with BAL-001 R1 and 2. Also, the justification should clarify the point of the discussion related to equating compliance based on

Organization	Yes or No	Question 2 Comment
		compliance of BAL-001 R 1 and 2 and how that argument justifies retirement. CIP-001-2a R4 - The justification statement should clarify that this requirement is redundant to the communications obligations in R1-3.CIP-003-3, 4 R1.2 - In addition to the justifications presented in the SAR, the term "readily available" is ambiguous and creates the opportunity for the use of CEA subjective judgment during compliance assessments. This is problematic for compliance risk generally, but is especially problematic when the requirement is administrative in nature. Entities should not be subject to unnecessary compliance risk based on ambiguity that can result in subjective compliance determinations based on the opinion of CEA personnel, as opposed to the four corners of the requirements, especially when the underlying requirement provides no reliability value. Further evidence that this requirement serves no purpose is the fact that it is not included in CIP v5. CIP-003-3 R3, 3.1, 3.2 and 3.3 - In addition to the justifications presented in the SAR, this issue is already fully addressed in the TFE process in Appendix 4D of the ROP, which is not only adequate, but is the appropriate place for this type of administrative function related to documentation. There are a specific set of defined requirements that allow an exception, and those exceptions have be to be filed according to the TFE process. Thus, the requirements proposed for retirement are redundant to that process. CIP-003-3, -4 R4.2 - In addition to the justification presented in the SAR, the phrase "based on sensitivity", is ambiguous and creates the opportunity to insert subjective judgment into compliance assessments. This is problematic for compliance risk generally, but especially when the requirement is administrative in nature AND redundant. Entities should not be subject to unnecessary compliance risk based on ambiguity resulting in subjective compliance determinations, as opposed to the four corners of the requirements, especially when the underlying requirement provides no operational reliability value. Further evidence that this requirement serves no purpose is the fact that it is not included in CIP v5. CIP-005-3a, -4a R2.6 - The justification statement could benefit from additional clarification as to why the banner is not useful. An appropriate use banner has not been useful over time, because people who intend to use sites inappropriately will simply ignore the

Organization	Yes or No	Question 2 Comment
		banner. Banners are generally considered to be a legal protection and not a security protection. Further evidence that this requirement serves no purpose is the fact that it has been removed from CIP v5 because the use of banners does not meet a reliability objective.CIP-007-3, -4 R7.3 - In addition to the justification presented in the SAR, it should be noted that to demonstrate that an entity performed the data destruction under R7.1 and R7.2, the entity needs to collect evidence. Having a separate requirement for evidence is redundant and not needed. COM-001-1.1 R6 - In addition to the justification presented in the SAR, the justification statement could note that this policy should be documented in the ROP for information within NERCNet that is considered sensitive or impacting to the BES. It should be a voluntary best practice or business practice for other information so that entities may use it, or use some other policy that better fits its circumstances. The justification should state that the NERCNet policy should be a voluntary best practice type of issue for information that is not considered sensitive or impacting to the BES. EOP-009-0 R2 - This is a reporting obligation and a documentation issue. The justification statement should also note that both documentation and reporting on this does not rise to the level of a reliability standard. The statement could note that this may be a best practices issue, but just for documentation. Reporting test results to REs isn't a best practice. Additionally, the justification should not state that the relevant information is better considered / obtained during an audit. If it's not relevant to the mandatory requirements, then it has no place in CMEP proceedings.FAC-002-1 R2 - The justification should not include that the relevant information is better considered / obtained during an audit. If it's not relevant to the mandatory requirements, then it has no place in CMEP proceedings.FAC-008-1 R1.3.5 - In addition to the justification presented in the SAR, the justification statement could note that the term "other assumptions" is ambiguous and introduces the potential for inefficient/ineffective administration of the CMEP due to introduction of subjectivity and opinions into compliance assessments. This is problematic for compliance risk generally, but especially when the requirement is administrative in nature AND redundant. Entities should not be subject to unnecessary compliance risk based on ambiguity resulting in

Organization	Yes or No	Question 2 Comment
		subjective compliance determinations, as opposed to the four corners of the requirements, especially when the underlying requirement provides no operational reliability value.FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5 - In addition to the justification presented in the SAR, the justification statement could note that it is inappropriate for entities other than the owners of equipment to establish facility ratings. The owners don't have to change their ratings, but the scheme is far more effective if the respective functional roles are distinct and not blurred by the review process contemplated in the requirements proposed for retirement. The owners should set the ratings and the RCs receive them and perform their functions in accordance with those ratings. The RC should not be involved with the TO/GO business-management of their equipment. Also, by keeping the roles distinct, it mitigates any liability risk of the third party if the owner uses its input and then the equipment breaks because of the new rating;FAC-013-2 R3 - Same comment as above.MOD-004-1 R1; MOD-004-1 R1.1; MOD-004-1 R1.2; MOD-004-1 R1.3; MOD-004-1 R2; MOD-004-1 R3; MOD-004-1 R3.1; MOD-004-1 R3.2; MOD-004-1 R4; MOD-004-1 R4.1; MOD-004-1 R4.2; MOD-004-1 R5; MOD-004-1 R5.1; MOD-004-1 R5.2; MOD-004-1 R6; MOD-004-1 R6.1; MOD-004-1 R6.2; MOD-004-1 R7; MOD-004-1 R8; MOD-004-1 R9; MOD-004-1 R9.1; MOD-004-1 R9.2; MOD-004-1 R10; MOD-004-1 R11; MOD-004-1 R12; MOD-004-1 R12.1; MOD-004-1 R12.2; MOD-004-1 R12.3 - ERCOT agrees with the comments/justifications.PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 - In addition to the justification presented in the SAR, the justification statement could note that the tasks required in these standards are administrative/documentation/reporting in nature and they don't affect reliability from a standards perspective. These could either be best practices or evidentiary in RSAWs - e.g. provide UFLS/UVLS program documentation - which could be relative to requirements that have actionable UVLS/UFLS requirements;TOP-001-1a R3 - ERCOT agrees with the justification with regard to the RC function, but the TOP standard also requires BAs/GOPs to follow the directives of the TOP, so the two relevant requirements are not apples to apples. Modification to one or the other

Organization	Yes or No	Question 2 Comment
		may be needed to ensure appropriate authority and corresponding obligation to follow that authority is reflected in one or the other standard, or both, but eliminate overlaps.TOP-005-2a R1 - ERCOT agrees with the justification. This should either be in the ROP or just via the ISN access process/agreement.VAR-002-WECC-1 R2; VAR-501-WECC-1 R2 - ERCOT agrees with the justification, but if the documentation/reporting are not relevant for the requirement, then the SAR should not suggest the REs should seek the info in CMEP proceedings, which should solely focus on compliance with the substance of the standards.
SERC EC Planning Standards Subcommittee	Yes	
Dominion	Yes	
Pepco Holdings Inc & Affiliates	Yes	
PPL Corporation NERC Registered Affiliates	Yes	
Tampa Electric Company	Yes	
Manitoba Hydro	Yes	
City of Garland	Yes	
Entergy Services, Inc.	Yes	
Wolverine Power Supply Cooperative, Inc.	Yes	
Central Husdon Gas & Electric	Yes	

Organization	Yes or No	Question 2 Comment
Corporation		
Tucson Electric Power	Yes	
CPS Energy	Yes	
Edison Mission Marketing & Trading	Yes	
Illinois Municipal Electric Agency	Yes	
Idaho Power Company	Yes	
City of Austin dba Austin Energy	Yes	
Transmission Agency of Northern California	Yes	
Kansas City Power & Light	Yes	

3. The subsequent phases of the P81 project are designed to identify all FERC-approved Reliability Standard requirements that could not be included in the Initial Phase due to the need for additional analysis or an editing of language. Please list any Reliability Standard requirements that you believe should be revised or retired in a subsequent phase, and include a brief supporting statement and citation to at least one element of Criterion B for each requirement listed.

Summary Consideration:

The P81 SDT is very appreciative of the time and effort the commenters spent developing their responses to Question 3. The commenters proposed numerous requirements for consideration in a subsequent phase, including requirements in BAL, CIP, INT, FAC, MOD, and PRC Reliability Standards, among others. As a general observation, the commenters suggested several ways to handle Reliability Standard requirements in the subsequent phases, including (i) retiring a requirement; (ii) modifying the requirement; (iii) changing the functional applicability of a requirement; and (iv) combining requirements or standards. Also, several commenters, such as ERCOT, Independent Electricity System Operator and SPP Standards Review Group requested the ability to raise additional Reliability Standard requirements during the subsequent phases. Given the level of interest in the subsequent phases of the P81 project, it is appropriate for the P81 SDT to carefully consider how best to propose a process for the subsequent phases. To some extent, ERCOT said it well:

"The SDT should establish a prospective process that provides adequate time and opportunity for entities to perform a meaningful review of remaining requirements to determine which additional requirements warrant retirement and to develop appropriate criteria, if relevant, that may be incremental to the ones proposed in this SAR, and to develop appropriate retirement justifications based on the relevant retirement criteria."

Consequently, while all the requests for consideration of Reliability Standard requirements in subsequent phases will receive consideration (including those requirements suggested for Phase I, but deferred to a subsequent phase), the process by which that consideration will be undertaken needs to be developed in light of the requirements suggested for subsequent phases. Accordingly, based on the comments, the P81 SDT intends to develop and suggest options to the Standards Committee in the near future on how to move forward with the subsequent phases.

Organization	Yes or No	Question 3 Comment
ACES Power Marketing		(1) EOP-002-3 R6 and R7 and their sub-requirements are redundant with BAL-001-

Organization	Yes or No	Question 3 Comment
Standards Collaborators		0.1a R1 and R2 and BAL-002 R4. BAL-001-0.1a R1 compels a BA to meet CPS1. BAL-001-0.1a R2 compels a BA to meet CPS2. BAL-002 R4 compels a BA to respond meet the DCS for all reportable events less than MSSC. EOP-002-3 R6 and R7 do not make the BA any more or less responsible to meet these requirements but rather creates an opportunity for double jeopardy. Furthermore, EOP-002-3 R6 and R7 do not make any sense in context with the CPS1 and CPS2 calculations. They are averages over a long term and would never require the emergency actions listed in the sub-requirements to comply with them. These requirements have already proven to incent behavior that is contrary to reliability (criterion B.8). At the August NERC BOT meeting, the NERC OC Chair explained that a BA shed load to meet the DCS criterion even though there were no other concerns (i.e. voltage, frequency, IROL or SOL violations) on the transmission system at the time. These requirements meet criterion B.7. (2) EOP-004-1 R2 should be considered for future retirement. The approval of the Event Analysis Procedure obviates the need for a standard requirement to analyze Bulk Electric System disturbances. This would be especially true if the procedure is added to the Rules of Procedure as NERC has planned. This requirement meets criterion B.7.(3) Retirement of FAC-001-0 R3 should be considered in the next phase. There is an implied obligation for the TO to update its Facility connection requirements when they change. Additionally, a requirement to make them available to the Regional Entity and users of the transmission system is unnecessary. First, the Regional Entity could request them through the compliance monitoring process. Second, the TO will provide the Facility connection requirements to those with genuine interconnection requests because the TO will want its connection standards met. This requirement meets criterion B.4, B.7 and B.9. (4) FAC-002-1 R1 should be revised to reflect the NERC Functional Model because it assigns the requirements to the wrong functional entities. The Transmission Planner and Planning Coordinator are responsible for conducting the assessments for new Facilities. The requirement appears to be an attempt to require the GO, TO, DP, and LSE to coordinate with the TP and PC. However, the requirement actually defines what is required in the TP and PC assessments which unfortunately place these

Organization	Yes or No	Question 3 Comment
		responsibilities on the GO, TO, DP and LSE. None of these functional entities have the capability to meet requirements such as performing dynamics studies. This requirement meets criterion B.8. (5) VAR-001-2 R2 and TOP-006-2 R2 are duplicate requirements. VAR-001-2 R2 compels the TOP to acquire sufficient reactive resources. TOP-006-2 R2 requires the RC, TOP and BA to monitor reactive resources. Since VAR-001-2 R2 applies all the time, a TOP cannot know they have acquired and maintained reactive resources unless they are monitoring them. Furthermore, TOP-006-2 R2 incorrectly applies to the BA. According to the NERC Functional Model, the BA cannot monitor reactive resources that are not generators and have no role in ensuring system voltages. Thus, TOP-006-2 R2 meets criterion B.7 because it is redundant, and it meets criteria B.8 and B.9 because it assigns responsibility to a functional entity (BA) that cannot meet it. This distracts the BA from its reliability mission.
Independent Electricity System Operator		(1) IRO-004-2 R1 could be retired if the wording in IRO-001-1.1 R8 was changed to cover all operating timeframes (Criterion B7). (2) We do not have any other particular standards/requirements in mind at this time. However, we will review and propose additional candidates for future phases as this project gets into the mid or end of Phase I. We believe the industry should focus on the Phase I effort at this time to gauge the regulator's and industry's reaction before marching too far down the path.
Western Electricity Coordinating Council		CIP 002 R2/R3/R4: Redundant and require revision. Each of these requirements requires an annual review of the Critical Asset list and Critical Cyber Asset list. WECC agrees these protections are required, however, the standard should be revised so either CIP 002-3 R4 is removed and CIP 002-3 R1-R3 are revised to require annual review and approval of the appropriate documentation, or CIP 002-3 R2 and R3 are revised to no longer require an annual review.CIP 005 R1.5/006 R3: These are redundant and should be removed/revised. CIP 006-3 R3 is redundant with CIP 005-3 R1.5. Either CIP 005-3 R1.5 should be revised to no longer require the protections of CIP 006-3 R3, or CIP 006-3 R3 should be removed and the content of CIP 006 R3 moved to CIP 005 R1.5.CIP 005 R1.5/006 R2.2: Redundant. Should be revised. Devices

Organization	Yes or No	Question 3 Comment
		applicable to these requirements may be redundant if they are classified as CCA (thus duplicated with CIP 002 - CIP 009) or reside within an ESP (thus duplicated with CIP 007). The requirements should be revised to take into account the situation where a device resides within an ESP or is classified as CCA, and is a device used in the EACM/PACM of ESPs/PSPs. Note: It appears this is being addressed in V.5 of CIP.CIP-005, R5: Should be removed and the protections highlighted in this requirement moved to appropriate requirements it references. This will cause less confusion with entities, and be more precise with exactly what documentation is required to be reviewed and approved.CIP 005 R5.1/R5.2: Redundant. Should revise CIP 005 R1.6 to include the wording of CIP 005 R5.1, and remove CIP 005 R5.1. This will cause less confusion with entities, and be better aligned with the CIP 005 R1.6 requirement.CIP 005 R5.3: Redundant. Should revise CIP 005 R3 to include the wording of this sub-requirement, and CIP 005 R5.3 should be removed. This change will create a better fit in the appropriate requirement, and be less confusing for entities.CIP 007 R9: Should be removed and the protections highlighted in this requirement moved to appropriate requirements it references. Thus CIP 007 requirements that require documentation should include the need to review and update the documentation. This will cause less confusion with entities, and be more precise with what documentation is required to be reviewed and approved.EOP-004-1 R3.2: Little, if any, value as a reliability requirement. This requirement points to attachments that could be addressed in the main part of the R3 standard. This requirement does nothing to promote the protection of the BES.VAR-001-2 R10: Redundant. The reliability purpose for R10 is to make sure that operators don't think that exceeding an SOL or IROL due to voltage issues is acceptable. There are multiple standards requiring operators not exceed and maintain an SOL or IROL with 30 minutes, regardless of the cause of the exceedance. These standards are TOP-001-2 R7, R11; TOP-004-2 R1; TOP-007-0 R2; TOP-008-1 R1.
Entergy Services, Inc.		CIP-006 R5 - A revision to the language in CIP-006 R5 is needed in order to require the review and handling of incidents of unauthorized access (when a door, gate or window has been opened without authorization), as opposed to what is more

Organization	Yes or No	Question 3 Comment
		accurately characterized as "unsuccessful" access attempts (e.g. invalid access card swipes). There currently is no definition of "unauthorized access attempts". The methods to be used for monitoring that are listed in the requirement, however do list: "Alarm Systems that alarm to indicate a door, gate or window has been opened without authorization". This method does not indicate that the alarm system must alarm on card swipes that do not result in the door opening, and be characterized as "Unauthorized Access attempts". Unsuccessful card swipes at a PSP access point, for example, do not suggest an unauthorized access attempt. A card swipe can be unsuccessful for a number of reasons, all of which are recorded by the key card system, such as the use of a deactivated card, an invalid card format, and a card not in the card file. An unsuccessful card swipe itself is not an indication that a PSP access point was “opened within authorization” because it does not indicate that the door has been opened in any manner. However, in the FAQ guidance for the CIP Reliability Standards, NERC acknowledged that Responsible Entities can consider single failed access attempts such as a single failed log-in not to be suspicious events requiring a response A single failed card swipe should be treated in the same way. The rewording of this requirement would address Criteria B-8 - "Hinders the protection or reliable operation of the BES." Investigating and documenting each unsuccessful card swipe would take a tremendous amount of time and produce a significant amount of paperwork without providing any additional physical security.CIP-005 R3 and CIP-006 R5 - Revisions to the wording around the timing of monitoring both physical and electronic access are needed. CIP-005 R3 - Monitoring Electronic Access states that "The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week." and CIP-006 R5 -Monitoring Physical Access stats that "The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in

Organization	Yes or No	Question 3 Comment
		Requirement CIP-008-3.The "twenty-four hours a day, seven days a week" portion of these requirements provides an unachievable requirement for 100% uptime for all systems used to monitor such access. The requirement should allow for a resonable amount of downtime. Either the "twenty-four hours a day, seven days a week" wording in these requirements could be removed altogether, or alternative langauge, such as requiring "High Availability" (for example 99.9% uptime) or some other wording that allowed for very small amounts of downtime that might be required for system reboots or minor maintenance.
SRC		Consider including the following standards for review in Phase II:BAL-004-0 - Time Error CorrectionMOD-030-2 - Flowgate MethodologyPRC-006-1 R8 (provision of data)PRC-006-1 R14 (administrative - response to written comments)
MidAmerican Energy Company		Consider the list provided by EEI.
Georgia System Operations Corporation		EOP-002-3, R1PER-001-0.1, R1Criteria B7, 9Statement: reference to BA or RC responsibilities and authority are within the criteria of NERC's Functional Model and so this is redundant. In addition, it is understood that these functions are substantial if not paramount for an entity to become certified as such. FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. All INT standardsCriteria B 1, 3 and 6Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Reliability Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Note: INT-007-1 R1.2 is part of Initial Phase. All data collection requirementsCIP-005-3a, 4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4; R7.3CIP-008-3, -4 R2PRC-018-1, R5Criteria B1,2 and 9Statement: These requirements are for data retention and although the need is

Organization	Yes or No	Question 3 Comment
		substancial, i.e. as a sort of forensic tool, they serve no function to reliability from an immediate time perspective.Standards currently requiring reporting.Criteria 1, 4 and 9EOP-002-3 R9.2EOP-004-1 R3 and its subrequirements; R4 and R5FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Statement: These are all reporting requirements; they do not aid reliability from an immediate time perspective. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards.Requirements applied to annual reviewsCriteria B1, 2,3 7 and 9CIP-002-2, -4 R4CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Statement: These requirements do not closely relate to operations of the Bulk Electric System. They would be better served as processes expected of entities to manage their compliance programs and processes. PRC-005-1b, R2Criteria B4, 9Statement: This requirement needs to be revised such that language is elminated as it refers to the entity providing to its RE within 30 days. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard.
Electric Reliability Council of Texas, Inc.		ERCOT agrees with the ISO/RTO SCR comments. However, in addition to the SRC comments, ERCOT offers the following:ERCOT supports future phases of the P81 project to eliminate/retire reliability standards that do not facilitate BES reliability. ERCOT is reviewing all standards to that end, however, developing a list of additional

Organization	Yes or No	Question 3 Comment
		requirements for retirement will require additional time. The SDT should establish a prospective process that provides adequate time and opportunity for entities to perform a meaningful review of remaining requirements to determine which additional requirements warrant retirement and to develop appropriate criteria, if relevant, that may be incremental to the ones proposed in this SAR, and to develop appropriate retirement justifications based on the relevant retirement criteria.
City of Austin dba Austin Energy		FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. Once an interconnection request is actually made with a transmission owner, the transmission owner performs the FAC-002-1 steady-state, short-circuit, and dynamics studies to determine the new interconnection's impact on reliability. During the negotiation of an interconnection agreement the FAC-001-0 referenced material is agreed on and reduced to writing for purposes of constructing, maintaining and operating the interconnection facilities. Also, during the entire interconnection process, as FAC-002-1 provides for, the parties must coordinate and cooperate during the assessment of the reliability impact of the new interconnection facilities. Thus, FAC-001-0, at best, is a best practice or helpful initial guide to an entity considering interconnecting, but provides little, if any, meaningful value to reliability, especially when compared to the actual benefits to reliability via the FAC-002-1 studies, the execution of a negotiated agreement and the coordination of activities during constriction and operation of the new facilities. Accordingly, FAC-001-0 should be retired, and, if necessary, any requirements that protect reliability should be transferred to FAC-002-1. All INT Standards Criteria B 6, 7 and 9Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Thus, we recommend that the Standards Drafting Team retire the INT Reliability Standards and, as necessary, transfer any requirement that protect

Organization	Yes or No	Question 3 Comment
		reliability to the BAL Reliability Standards. All data collection requirements not included in the Initial Phase, more specifically:CIP-005-3a, -4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4CIP-008-3, -4 R2PRC-018-1 R5Criteria B 1, 2 and 9Statement: These requirements are purely data retention requirements with no functional nexus to reliability and, therefore, best handled via compliance monitoring, RSAW or as a data request during an audit. All reporting out requirements not included in the Initial Phase, more specifically:EOP-002-3 R9.2EOP-004-1 R3 and its subrequirements; R4 and R5FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Criteria B 1, 4 and 9Statement: There is no direct connection between reporting out of information to an entity or Regional Entity and protecting reliability. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards.Annual reviewsCIP-002-3, R3; CIP-002 -4 R3CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Criteria B 1, 2, 3, 7 and 9Statement: The annual review and update requirements are arbitrary, administrative and not aligned with the operation and protection of the Bulk Electric System. These requirements should be retired or modified to align with how the Bulk Electric System is operated and protected. Other requirementsCIP-007-3, -4 R7 Criteria B 1, 2, 3 and 7Statement: The essential elements of the process of disposing or redeploying of Cyber Assets and the associated cyber security are set forth in R7.2 and R7.3. To require “formal methods, processes and procedures” appears to require formal documentation for the sake of documentation, rather than allowing the responsible entity to implement a process that achieves the actions required in R7.2 and R7.3,

Organization	Yes or No	Question 3 Comment
		which may or may not include formal procedures, for example. EOP-004-1 R2Criteria B 7 Statement: The analysis of the BES for system disturbances is covered in PRC-004-2.1a R1. The PRC Requirement R1 calls for the analysis of its transmission Protection System Misoperations. We believe that BES analysis is covered inherently through this PRC standard making EOP-004 R1 redundant to the PRC standard.Another factor is the Version 2 of the EOP-004-2 where the requirement to analyze the BES disturbance is noticeably absent. The focus on the EOP-004 is for the reporting of applicable events that are identified in the PRC-004 standard. There is an event analysis reporting process referenced in the NERC Rules of Procedures (ROPs) that handles this requirement. Therefore, this is a redundant requirement. In February of 2012, NERC deployed its Events Analysis Process - incorporating the learnings from two field trials held over the previous year and a half. It includes all the necessary steps that affected operators must take to analyze and report on events that may impair the reliability of the BES. Most Regional Entities have already updated their reporting procedures to match NERC's. Furthermore, NERC and the Regional Entities already have sufficient authority to order analyses and corrective action plans outside of the Reliability Standards. These are important steps for the development of Lessons Learned and trending analyses, but do not contribute to reliable operations. In fact, the demand for near term reporting - some within one hour of the initiation of the event - interferes with the efforts of front-line personnel to mitigate the issue at handBAL-001-0.1a (all requirements), BAL-004-0 (all requirements), BAL-005-0.1b R11; BAL-006-2 (all requirements)Criteria B 6 and 9Statement: BAL-001 requires a 12 month rolling average of ACE and does not impact reliability and should be eliminated (in favor of BAL-002). Consider augmenting NAESB standard WEQ-005.BAL-004 requirement for time error correction is not important for reliability and should be eliminated. It also duplicates NAESB std WEQ-006.In BAL-005 R11, Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE, is not needed for reliability. Ramp rates have minimal impact on ACE calculations, and are already included in the

Organization	Yes or No	Question 3 Comment
		definition of Interchange Schedule in the NERC Glossary as used in R9. The requirement to use agreed upon ramp rates is commercial in nature and is already covered by NAESB standard WEQ-004-17.BAL-006-2 is an after-the-fact accounting of inadvertent interchange and does not impact reliability and should be eliminated. Consider augmenting NAESB standard WEQ-007.CIP-003-3, -4 R2 and its subrequirementsCriteria B 1 and 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is an employee called a CIP senior manager oversees the plan. CIP-004-3, -4 R2.3 Criteria B 9Statement: Whether the entity has a robust up-to-date, trained-on CIP compliance plan may impact reliability, but not whether there is annual training. CIP-004-3, -4 R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is a seven year update to the PRA. CIP-004-3, -4 R4.1Criteria B 1, 9Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it reviews lists every seven days. CIP-004-3, -4 R4.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it revokes access within 24 hours or 7 days. CIP-005-3a, -4a R2.5 and its subrequirementsCriteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the ESP may impact reliability, but not whether specific information is documented. CIP-007-3, -4 R3.1, R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented within 30 days. Also, whether the entity has a robust up-to-date on CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented. CIP-008-3 R1.4Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether specific information is documented within 30 days or a change. EOP-001-1b, -2bCriteria B 7Statement: Duplicative with the other EOP Standards (e.g., Capacity and Energy emergency of EOP-002, Load Shedding of EOP-003, and System Restoration of EOP-005).EOP-002-3 R1Criteria B 7Statement: Duplicates other

Organization	Yes or No	Question 3 Comment
		requirements such as IRO-001-1 R8 and should be retired or modified to reduce redundancy. EOP-002-3 R9 Criteria B 7Statement: When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources). It duplicates NAESB standard WEQ-008 and should be eliminated.EOP-005-2 R1.2.A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration. Criteria B 1, 3 and 7 Statement: With the implementation of NUC-001-2 R2, there is no longer a need for EOP-005-2 R1.2. Specifically, NUC-001-2 R2 requires Nuclear Plant Interface Requirements (NPIRs) to be included in the agreements for operation and maintenance (including restoration process) for off-site nuclear power:R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements1 that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.Given the off-site power requirements of NUC-001-2 which require comprehensive operational interface protocols (including restoration) between nuclear plants and responsible entities as part of the NPIRs, there is no longer a need for the administrative, documentation-only requirement in EOP-005-2 related to the same subject matter.IRO-002-2 (all requirements)Criteria B 7Statement: Redundant with COM-002-2, R1 COM-001-1.1, R1 and IRO-002-2, R2 and R3IRO-005-3a R10Criteria B 9Statement: Confusing requirement. It was intended to address rare cases where entities were told to operate to different SOLs and IROLs. However, because only the TOP and the RC can see these parameters, the only thing a GOP can do is follow a directive.IRO-014-1 R4Criteria B 9Statement: Requirement 4 (including sub-parts) should be rolled up into R1. and eliminated. Requirement 1 should be modified to require "current operating procedures, processes or plans with all adjacent RCs.IRO-015-1 R2.1Criteria B1 and 9Statement: Whether the procedure, process and plan is

Organization	Yes or No	Question 3 Comment
		robust and up-to-date may impact reliability, not whether there are weekly calls.MOD-001-1 and MOD-008-1 (all requirements)Criteria 6 and 9Statement: Do the ATC / TTC standards belong in NERC or NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? I think NERC should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., and I think these can/should be moved to the NAESB standards.Criteria B 6 and 9Statement: This could be handled as a data request from an RE or other Registered Entities and, therefore, would not need a requirement, as there are too many requirements that warrant an attestation that no request was made.MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard.MOD-028-1 (all requirements); MOD-029-1a (all requirements); MOD-030-2 (all requirements)Criteria B 6 and 9Statements: ATC / TTC standards should belong NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? NERC should focus on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc.PRC-022-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.5Criteria B 7Statement: Whether the responsible entity has robust UVLS misoperation and correction action is redundant with PRC-004-1a, -2a. TOP-001-1a R3 and R7 (and its subrequirements)Criteria B 9Statement: For R3, there are three projects in progress addressing the issuance of directives by the RC, BA and TOP. Also, for R7, all outages information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R8 and R 9Criteria B 6, 7 and 9Statement: “Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency”, duplicates VAR-001 and should be eliminated. “Each Balancing Authority shall plan to meet Interchange Schedules and ramps” duplicates the BAL standards and the NEASB standards and should be eliminated.TOP-002-2b R12Criteria B 6 and 9Statement: ATC / TTC standards should belong to NAESB (i.e., MOD-001, MOD-004, MOD-008,

Organization	Yes or No	Question 3 Comment
		MOD-028 thru 030, and TOP-002-2 R12). NERC should focus on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., These can/should be moved to the NAESB standard.TOP-002-2b R14 and R14.1Criteria B 9Statement: All derating information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R15Criteria B 9Statement: Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations is a "how" requirement that is needed to meet other requirements in the standard. It is also not measureable, and the requirement should be eliminated. All weekly forecasts should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-003-1 R1 and its subrequirements; R2 and R3Criteria B 9Statement: All planned outage information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-005-2a R3Criteria B 9Statement: PSEs are not best positioned to provide reliability information.BAL-005-0.1b R1Criteria B7Statement: Introductory statement; redundant with subrequirements MOD-010-0 R2Criteria B 1, 4 and 9Statement: MOD-012-0 R2 was included in the Joint Trade Associations list of suggested requirements for retirement or modification. MOD-010-0 R2 is nearly identical to MOD-012-0 R2 and should also be considered.PER-001-0.1 R1Criteria B7Statement: The TOP portion of this requirement is redundant with TOP-001-1a R1PRC-018-1 R3 (and all sub requirements)Criteria B2 and 4Statement: This requirement involves data collecting and reporting that does not impact the reliability of the BES; could be part of a data request if necessary
Georgia Transmission Corporation		FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria Meets Criteria A and a combination of either or all of B1, B2, B3, B4, B 9Statement: MOD-016 through MOD-021 are about long term load forecasting and reporting of actual and forecast loads. Requirements could be eliminated from the standards and replaced with a data collection process (e.g.,

Organization	Yes or No	Question 3 Comment
		TADS/DADS, etc.). Loads to be used in modeling could be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard. Additionally, MODs-016 through 021 have yet to be classified as Tier 1, 2, or 3; nor have they yet to be identified on NERC's Actively Monitored List.PRC-006-1 (R7, R8, and R14) Criteria: Meets Criteria A and a combination of either or all of B1, B3, B4, B9Statement: Recommend these requirements to be eliminated from the standards and replaced with a data collection and or reporting process (e.g., TADS/DADS, etc.). PRC-023-1 (R3.3) Criteria: Meets Criteria A and a combination of either or all of B1, B4, B9Statement: Recommend these requirements to be eliminated from the standards and replaced with a data reporting process.TOP-001-1a (R4) Criteria: Meets Criteria A and B1Statement: Same requirement as TOP-001-1a (R3) which made the Phase I list, only difference is applicability.
Occidental Power Services, Inc.		If the changes listed in Question 2 are not considered in Phase 1, then they should be considered in subsequent phases of the project.
Illinois Municipal Electric Agency		IRO-010-1a R3
Idaho Power Company		MOD-017-0.1 R1.1, R1.2 Criterion B2MOD-018-0 R1 Criterion B7 (Should be covered by MOD-016)MOD-021-1 R1, R2 Criterion B7 (Should be covered by MOD-016)MOD-021-1 R3 Criterion B4
CPS Energy		No additional comments.
Salt River Project		No additions at this time.
Occidental Energy Ventures Corp.		OEVC agrees with the process that the Trades are using to approach this question, but do not agree with some of their priorities. OEVC has only addressed the Requirements where OEVC has additional comments to what the Trades have provided.In addition, OEVC believes the following requirements can also be

Organization	Yes or No	Question 3 Comment
		removed:a) BAL-005, R1.1 - BA metering is financial in nature. Telemetry is already required for reliability.b) TOP-002, R13 - Generator validations are driven by the regions already.FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: OEVC agrees with the Trade's analysis, but will also point out that once connection requirements are in place, they will rarely change. We believe this would mean a lower priority is in order. All INT Standards Criteria B 6, 7 and 9 Statement: Again, OEVC agrees with the Trades on this. It may even be time to suggest that the functional designation of the PSE go away. They serve a marketing purpose and are blind to reliability indicators. All data collection requirements not included in the Initial PhaseCIP-005-3a, -4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4; R7.3CIP-008-3, -4 R2PRC-018-1 R5Criteria B 1, 2 and 9 Statement: OEVC agrees with the Trades. Most of these are captured in Phase I. These fit in the same category. All reporting out requirements not included in the Initial PhaseCIP-001-2a R3 should be modified to eliminate the word "reporting" (added by OEVC)EOP-002-3 R9.2EOP-004-1 R3 and its sub requirements; R4 and R5 FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-010-0 R2 Similar to MOD-012-0 (added by OEVC)MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Criteria B 1, 4 and 9 Statement: In addition to the Trade's comments, OEVC believes that NERC has an Events Analysis process, RAPA process, and Section 1600 Data Request process that they can invoke to get this information.Annual reviewsCIP-002-2, -4 R4CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Criteria B 1, 2, 3, 7 and 9 Statement: OEVC agrees with the Trades and add that Compliance teams spend far too much time trying to confirm that a RBAM was reviewed and signed off-on. This serves only to add time and expense - especially when conditions have not changed in the preceding year.

Organization	Yes or No	Question 3 Comment
		Other requirements EOP-004-1 R2 Criteria B 7 Statement: OEVC agrees with the Trades. Again, NERC has an Events Analysis process and RAPA process that they can invoke to require analyses. FAC-002-1 R1OEVC agrees that this requirement and five sub-requirements are unnecessary. First of all, the PUC, the BA, and the TOP are highly involved in the interconnection process. It is not clear what extra value is provided by overlapping oversight from the RE and/or NERC. Second, other standards - the TPLs in particular - are directly referenced in the requirement. Those are enforceable already, there is no need to duplicate them here.FAC-008-1 R1.3.5This requirement is already addressed in Phase I.IRO-001-1.1 R8 OEVC believes the intent is to consolidate RC directives in IRO-001 with TOP directives in TOP-001. Since Phase I addresses TOP-001, this seems to have been already accomplished.IRO-005-3a R10Criteria B 9Statement: OEVC agrees with the Trades. This is one that we propose should be a much higher priority. Since the GOP is already told to follow a directive, this requirement makes no sense. MOD-017-0.1 R1.1 and MOD-018-0 (all requirements) ; MOD-020-1 R1OEVC believes that this is redundant with IRO-010 and the new version of TOP-003 when it takes effect.MOD-019-0.1 R1OEVC believes that this is redundant with IRO-010 and the new version of TOP-003 when it takes effect. TOP-002-2b R2; R15OEVC believes that TOP-002 R15 will be resolved by the release of the new TOP standards.TOP-002-2b R14 and R14.1Criteria B 9Statement: OEVC believes that TOP-002 R14 and R14.1 will be resolved by the release of the new TOP standards.TOP-003-1 R1 and its sub requirements; R2 and R3Criteria B 9Statement: OEVC believes that these items will be resolved by the release of the new TOP standards.TOP-005-2a R3Criteria B 9Statement: OEVC agrees with the Trades on this one. Again, it may even be time to suggest that the functional designation of the PSE go away. TOP-006-2 R1.1, R4, R5, R6; TOP-008-1 R2, R4 OEVC believes that that TOP-006 R1.1 will be resolved by the release of the new TOP standards.
NERC Staff Technical Review		Please see NERC Staff's response to question 2 for Phase I requirements that NERC Staff recommends be reviewed for inclusion in a future phase. NERC Staff may propose additional requirements for a future phase of the P81 project at a later date.

Organization	Yes or No	Question 3 Comment
American Electric Power		Please see the response to Question #2 for additional Reliability Standard requirements that AEP would like to be considered as candidates for retirement on this initial, or subsequent, request for comment.
seattle city light		Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Tampa Electric Company		Tampa Electric suggests that the P81 Drafting Team consider the adoption of concepts from the CIP version 5 criteria for consideration under CIP version 3 and 4. In particular Tampa Electric proposes that draft language for CIP-007 patching will reduce administrative burden for compliance with patching process TFEs under current versions (CIP-007 V3 and V4). The version 5 draft Guidelines and Technical Basis for CIP-007 V5 states: R2.1 A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. R2.2 Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.
Manitoba Hydro		The following statement should be removed from the standard as it does not support reliability of the BES [B8]:FAC-013-2 R5. 'However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request'The following statement should be removed from the standard as it does not support reliability or provide any protection to the BES. [B8]:FAC-013-2 R6. 'If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to

Organization	Yes or No	Question 3 Comment
		that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information'.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade Associations).		The Trade Associations support the following list of Reliability Standard requirements to be retired or modified in a subsequent phase of the P81 project. To assist the Standards Drafting Team decide what should be considered in phase 2, phase 3 etc., the Trade Associations have listed the requirements in the order of importance - with those at the top of the list candidates for phase 2. The Trade Associations understand, however, that the decision on how best to proceed with phase 2, phase 3 will be weighed by the Standards Drafting Team, and, therefore, have not indicated any bright line on what should or should not be included in phase 2 versus phase 3, etc. The Trade Associations further note that the list of requirements listed below may be supplemented with additional requirements as the phase 2/phase 3 discussions evolve. Additionally, the Trade Associations believe that additional criteria for elimination may be proposed as part of the phase 2/phase 3 process.FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. Once an interconnection request is actually submitted to a transmission owner, the transmission owner performs the FAC-002-1 steady-state, short-circuit, and dynamics studies to determine the new interconnection's impact on reliability. During the negotiation of an interconnection agreement the FAC-001-0 reference material is agreed on and reduced to writing for purposes of constructing, maintaining and operating the interconnection facilities. Also, FAC-002-1 imposes an obligation on the parties to coordinate and cooperate during the assessment of the reliability impact of the new interconnection facilities. Thus, FAC-001-0, at best, is a best practice or helpful initial guide to an entity considering interconnecting, but provides little, if any, meaningful value to reliability, especially when compared to the actual benefits to reliability via the FAC-002-1

Organization	Yes or No	Question 3 Comment
		studies, the execution of a negotiated agreement and the coordination of activities during construction and operation of the new facilities. Accordingly, FAC-001-0 should be retired, and, if necessary, the transfer of any requirements that protect reliability to FAC-002-1. All INT Standards (With the exception of INT-007-1 R1.2 which is part of and should remain in the Initial Phase.)Criteria B 6, 7 and 9 Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Reliability Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Thus, it is recommended that the Standards Drafting Team retire the INT Reliability Standards, and, as necessary, transfer any requirement that protect reliability to the BAL Reliability Standards. ALL DATA COLLECTION REQUIREMENTS NOT INCLUDED IN THE INITIAL PHASECIP-005-3a, -4a R5.3CIP-006-3c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4CIP-008-3, -4 R2PRC-018-1 R5Criteria B 1, 2 and 9Statement: These requirements are purely a data retention requirement with no functional nexus to reliability, and, therefore, are best handled via compliance monitoring, RSAWs or as a data request during an audit.ALL REPORTING OUT REQUIREMENTS NOT INCLUDED IN THE INITIAL PHASEEOP-002-3 R9.2EOP-004-1 R3 and its subrequirements; R4 and R5FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2; PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Criteria B 1, 4 and 9Statement: There is no direct nexus between reporting out of information to an entity or Regional Entity and protecting reliability. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards.Annual reviewsCIP-002-3, R3; CIP-002 -4 R3CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4

Organization	Yes or No	Question 3 Comment
		R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Criteria B 1, 2, 3, 7 and 9Statement: The annual review and update requirements are arbitrary, administrative and not aligned with the operation and protection of the Bulk Electric System. These requirements should be retired or modified to align with how the Bulk Electric System is operated and protected. OTHER REQUIREMENTSCIP-007-3, -4 R7 Criteria B 1, 2, 3 and 7Statement: The essential elements of the process of disposing or redeploying of Cyber Assets and the associated cyber security are set forth in R7.2 and R7.3. To require "formal methods, processes and procedures" appears to require formal documentation for the sake of documentation, rather than allowing the responsible entity to implement a process that achieves the actions required in R7.2 and R7.3, which may or may not include formal procedures, for example. EOP-004-1 R2Criteria B 7 Statement: The analysis of the BES for system disturbances is covered in the PRC-004-2.1a R1. The PRC Requirement R1 calls for the analysis of its transmission Protection System Misoperations. We believe that BES analysis is covered inherently through this PRC standard, making EOP-004 R1 redundant to the PRC standard. Another factor that was considered is the notable absence of any requirement in EOP-004-2 to analyze the BES disturbance. The focus of EOP-004 is on the reporting of applicable events that are identified in the PRC-004 standard. There is an event analysis reporting process referenced in the NERC Rules of Procedures (ROP) that addresses this requirement. Therefore, this is a redundant requirement. In February of 2012, NERC deployed its Events Analysis Process - incorporating the learnings from two field trials held over the previous year and a half. It includes all the necessary steps that affected operators must take to analyze and report on events that may impair the reliability of the BES. Most Regional Entities have already updated their reporting procedures to match NERC's. Furthermore, NERC and the Regional Entities already have sufficient authority to order analyses and corrective action plans outside of the Reliability Standards. These are important steps for the development of Lessons Learned and trending analyses, but do not contribute to reliable operations. In fact, it is arguable that the demand for near term reporting - some within one hour of the

Organization	Yes or No	Question 3 Comment
		initiation of the event - interferes with the efforts of front-line personnel to mitigate the issue at hand BAL-004-0 (all requirements), BAL-005-0.1b R11; BAL-006-2 (all requirements)Criteria B 6 and 9Statement: BAL-004 requirement for time error correction is not important for reliability and should be eliminated. BAL-004 also duplicates NAESB standard WEQ-006.BAL-005 R11 states that Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE. This requirement is not needed for reliability. Ramp rates have minimal impact on ACE calculations, and are already included in the definition of Interchange Schedule in the NERC Glossary as used in R9. The requirement to use agreed upon ramp rates is commercial in nature and is already covered by NAESB standard WEQ-004-17.BAL-006-2 is an after the fact accounting of inadvertent interchange and does not impact reliability and should be eliminated. Consider augmenting NAESB standard WEQ-007. CIP-003-3, -4 R2 and its subrequirementsCriteria B 1 and 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is an employee called a CIP senior manager that oversees the plan. CIP-004-3, -4 R2.3 Criteria B 9Statement: Whether the entity has a robust up-to-date, trained-on CIP compliance plan may impact reliability, but not whether there is annual training. CIP-004-3, -4 R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is a seven year update to the personnel risk assessment(PRA). CIP-004-3, -4 R4.1Criteria B 1, 9Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it reviews lists every seven days. CIP-005-3a, -4a R2.5 and its subrequirementsCriteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the ESP may impact reliability, but not whether specific information is documented. CIP-007-3, -4 R3.1, R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented within 30 days. Also, whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but

Organization	Yes or No	Question 3 Comment
		not whether specific information is documented. CIP-008-3 R1.4Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether specific information is documented within 30 days or a change. EOP-001-1b, -2bCriteria B 7Statement: Duplicative with the other EOP Standards (e.g., Capacity and Energy emergency of EOP-002, Load Shedding of EOP-003, and System Restoration of EOP-005).EOP-002-3 R1Criteria B 7Statement: Duplicative of other requirements such as IRO-001-1 R8, and should be retired or modified to reduce redundancy. EOP-002-3 R9 Criteria B 7Statement: When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources). It is duplicative of NAESB standard WEQ-008 and should be eliminated.EOP-005-2 R1.2.A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration. Criteria B 1, 3 and 7 Statement: With the implementation of NUC-001-2 R2, there is no longer a need for EOP-005-2 R1.2. Specifically, NUC-001-2 R2 requires Nuclear Plant Interface Requirements (NPIRs) to be included in the agreements for operation and maintenance (including restoration process) for off-site nuclear power:Ref: NUC-001-2 R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements1 that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.Given the off-site power requirements of NUC-001-2 which require comprehensive operational interface protocols (including restoration) between nuclear plants and responsible entities as part of the NPIRs, there is no longer a need for the administrative, documentation-only requirement in EOP-005-2 related to the same subject matter.FAC-013-1 (all requirements)Criteria B 6Statement: It is really a commercial planning practice suitable for Order 1000 under Section 205/206 as opposed to Section 215.IRO-002-2 (all requirements)Criteria B

Organization	Yes or No	Question 3 Comment
		7Statement: Redundant with COM-002-2, R1 COM-001-1.1, R1 and IRO-002-2, R2 and R3IRO-005-3a R10Criteria B 9Statement: Confusing requirement. It was intended to address rare cases where entities were told to operate to different SOLs and IROLs. However, since only the TOP and the RC can see these parameters, the only thing a GOP can do is follow a directive.IRO-014-1 R4Criteria B 9Statement: Requirement 4 (including sub-parts) should be rolled up into R1 and eliminated. Requirement 1 should be modified to require "current operating procedures, processes or plans with all adjacent RCs.IRO-015-1 R2.1Criteria B1 and 9Statement: Whether the procedure, process and plan is robust and up-to-date may impact reliability, not whether there are weekly calls. MOD-001-1 and MOD-008-1 (all requirements)Criteria B 6 and 9Statement: NERC should be focused on modeling the BES and managing SOLs and IROLs, the methodologies for the determination of CBM, TTC and ATC are commercial matters associated with the reservation and allocation of rights to transfer capability among transmission customers. While transfer capability calculations should be based on models of the BES, the NAESB WEQ should address the issues raised in MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12.Criteria B 6 and 9Statement: This could be handled as a data request from an RE or other Registered Entities, and therefore would not need a requirement, as there are too many requirements that warrant an attestation that no request was made.MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard.MOD-019-0.1 R1Criteria B 1, 2, and 9Statement: MOD-019-0.1 covers “Reporting of Interruptible Demands and Direct Control Load Management,” which requires reporting of a forecast of interruptible demand and direct control load management data. This reporting is administrative in nature, and the information is not important for reliability. The data is best gathered through DADS and not through a standard.MOD-028-1 (all requirements); MOD-029-1a (all requirements);

Organization	Yes or No	Question 3 Comment
		MOD-030-2 (all requirements)Criteria B 6 and 9Statement: Do the ATC / TTC standards belong in NERC or NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? I think NERC should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., and I think these can/should be moved to the NAESB standards. PRC-011-0 R1 Criteria B 4 and 9Statement: Requirements for maintenance of under-frequency load shedding systems ("UFLS") and under-voltage load shedding systems ("UVLS") are not needed to meet an adequate level of BES reliability. UFLS and UVLS installations are widely distributed. Distribution circuit outages, distribution field switching, and varying load profiles, such as peak and off-peak, could impact the amount of load that would be automatically shed by UFLS and UVLS. Therefore, entities must include adequate margins above their obligation to be able to meet the obligated load shed at all times as required by Reliability Standards, such as PRC-006 and PRC-007, that are performance-based, or results-based. While UFLS and UVLS are, of course, important safety-net systems, PRC-011-0 R 1 maintenance requirement is not needed to provide a "defense-in-depth" approach due to the margins required to meet performance-based requirements. Thus, Like PRC-008-0 R1 included in Phase I, Reliability Standard PRC-011-0 R1 which involves maintenance of UVLS, is not needed. In fact, it is typically the same relays and associated equipment that provides both the UFLS and the UVLS functions. PRC-022-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.5Criteria B 7Statement: Whether the responsible entity has robust UVLS misoperation and correction action is redundant with PRC-004-1a, -2a. TOP-001-1a R7 (and its subrequirements)Criteria B 9Statement: For R3, there are three projects in progress addressing the issuance of directives by the RC, BA, and TOP. This includes COM-003-1's requirements for the issuances of "not quite directives" Also, for R7 All outages information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R8 and R 9Criteria B 6, 7 and 9Statement: "Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency", is duplicative of VAR-001 (and incorrect) and should be eliminated. "Each Balancing Authority shall plan to meet Interchange Schedules and ramps", is duplicative of the

Organization	Yes or No	Question 3 Comment
		BAL standards and the NAESB standards and should be eliminated.TOP-002-2b R12Criteria B 6 and 9Statement: The ATC / TTC standards may belong in NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? NERC standards should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc.TOP-002-2b R14 and R14.1Criteria B 9Statement: All derating information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R15Criteria B 9Statement: Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations is a "how" requirement that is needed to meet other requirements in the standard. It is also not measureable, and the requirement should be eliminated. All weekly forecasts should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-003-1 R1 and its subrequirements; R2 and R3Criteria B 9Statement: All planned outage information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-005-2a R3Criteria B 9Statement: PSEs are not best positioned to provide reliability information.
SPP Standards Review Group		VAR-002 R3 Status changes on AVRs - Quite often status changes to AVRs may be made for only a matter of seconds. These changes do not impact the reliability of the BES but still require a call be made for notification of the change. Perhaps the requirement could be changed such that only status changes which impact the BES need to be reported. This hits on Items 4, 5, 8 and 9 in Criterion B.FAC-003-1 R1.3 - Specific training is required for personnel involved with vegetation management programs. This requirement is purely administrative (Criterion B.1) and does not, in and of itself, benefit the reliability of the BES. (Although this requirement has been removed in subsequent versions of this standard (FAC-003-2 and FAC-003-3), it remains in effect today. It needs to be retired.)While we don't have an extensive list at this time, we would hope that the drafting team will ask for potential candidates which fit this category at some point in the future prior to the start of work on the latter phases of the project.

Organization	Yes or No	Question 3 Comment
Ameren		We support and agree with Trade Association's comments and their suggested list of Reliability Standard requirements to be retired or modified in the subsequent phase of the P81 Project. In addition, we suggest that IRO-005-3, R10 should be modify to eliminate its applicability to LSE and PSE in addition to GOP. While the IRO-005-3_1a, R10 is necessary for the reliable operation of the BES, its applicability to LSE and PSE also is questionable as these entities do not "operate" the BES. We believe that it is redundant (criteria B7) with other requirements where these entities (GOP, LSE, and PSE) have to follow the RC and/or TOP directives.
Wolverine Power Supply Cooperative, Inc.		Wolverine agrees with the list of requirements that the trade associations are submitting. We are a member of NRECA and agree with their comments.

4. If you have any other comments or suggestions on the draft SAR that you have not already provided in response to the previous questions, please provide them here.

Summary Consideration:

Comment

NERC staff requests that the scope of the SAR include currently-pending versions of related Reliability Standards to address requirements proposed in Phase I that are also included in a subsequent version of the standard that has been adopted by the NERC Board of Trustees, but not yet approved by FERC. Manitoba Hydro has a similar concern. NERC staff also requests that technical justifications only rely on Commission-approved Reliability Standards and how removal of a requirement will "increase in efficiency of the ERO compliance program" consistent with the language of P81.

Response

The P81 SDT added a footnote to the SAR to address how pending versions of related Reliability Standards (i.e., NERC BOT adopted) are considered so that eliminated requirements carry through to any new NERC BOT adopted versions. In addition, the P81 SDT is developing a technical white paper that it believes will provide a sound, technical basis for removal of each NERC Reliability Standard requirement proposed in Phase I. As appropriate, the technical basis will only reference or rely on Commission-approved Reliability Standards. The technical white paper being developed by the P81 SDT will generally address the issue of efficiency gains in the ERO compliance program with a blanket statement, on a requirement basis, or a combination of both.

Comment

Kansas City Power & Light states that the retirement of the requirements should not have a ripple impact in other standards or requirements.

Response

Although it is unclear to the P81 SDT what is meant by the term "ripple impact," it is believed to be similar to Criterion C's defense in depth concept. In the future, it would be helpful to provide some examples where the removal of a NERC Reliability Standard requirement may have a ripple impact in other standards. At this time, the P81 SDT believes the consideration of Criterion C (specifically, the consideration of whether retiring a requirement will have any negative impact on the defense-in-depth protection of the BES) ensures that other standards and requirements are not negatively impacted.

Comment

Entergy Services, Inc. states that during future phases industry input should be gathered in a more formal process. PPL Corporation NERC Registered Affiliates had a similar suggestion to increase stakeholder involvement.

Response

The P81 SDT is using the approved Standard Process Manual (SPM) for Phase I, and, at this point, plans to use the SPM in effect at the time for future phases of this project as well. The SDT acknowledges that stakeholder input may need to be gathered in a manner differently in subsequent phases than that used for Phase I, as subsequent phases may be more involved than simply removing requirements in their entirety and will likely require combining and/or re-wording of existing requirements.

Comment

Dominion observed some highlighting and number issues in the draft documents and appears to suggest we add IRO-001-1a R8.

Response

Requirement 8 of NERC Reliability Standard IRO-001-1a, while redundant to TOP-001-1a R3 with regard to Reliability Coordinators, will need to remain to ensure that a NERC Reliability Standard exists that addresses the need for entities to comply with a Reliability Coordinator's Reliability Directives.

Typographical errors will be addressed by the SDT.

The spreadsheet with proposed retirements on the NERC website will be manually sorted to ensure appropriate ordering of requirements on future revisions.

Comment

South Carolina Electric and Gas states that instead of retiring R2 of EOP-009-0 could the whole standard can be replaced by the new EOP-005?

Response

Yes, it is the SDT's understanding that NERC Reliability Standard EOP-009-0 will be retired when Standard EOP-005-2 becomes enforceable (July 1, 2013).

Comment

Idaho Power Company, among other things, suggests the combing of MOD standards 016 through 021.

Response

The suggested combining of NERC Reliability Standards MOD-016 through MOD-021 has been referred to the Question 3 sub-team for consideration for Phase II.

Comment

ACES Power Marketing Standards Collaborators and Electric Reliability Council of Texas, Inc. state that NERC needs to develop guidance that includes these criteria for drafting teams to avoid developing requirements that offer little reliability value in the future.

Response

The P81 SDT agrees that NERC-developed guidance is needed for standard drafting teams to ensure that new requirements consider the criteria established by the P81 SDT. The P81 SDT will address this issue with the NERC Standards Committee.

Comment

Georgia System Operations Corporation and Georgia Transmission Corporation suggest the consideration of requirements for retirement that supports NERC programs other than the mandatory Reliability Standards.

Response

The SDT appreciates the comments. The SDT believes that the criteria, as drafted, should capture those requirements that Georgia System Operations Corporation and Georgia Transmission Corporation are concerned about.

Organization	Yes or No	Question 4 Comment
NERC Staff Technical Review		(1) NERC Staff notes that the scope of the SAR should be expanded to include currently-pending versions of related Reliability Standards to address requirements proposed in Phase I that are also included in a subsequent version of the standard that has been adopted by the NERC Board of Trustees, but not yet approved by FERC. NERC Staff suggests that footnotes could be included to capture these situations.(2) NERC Staff submits that the technical justification for removal of particular requirements should not be a restatement of the Criteria (see e.g., INT-007-1 R1.2). Nor should the technical justifications reference and/or rely upon for support any Reliability Standards unless those Reliability Standards are Commission-approved. (3) NERC Staff suggests that the technical justifications for the satisfaction of the Criteria

Organization	Yes or No	Question 4 Comment
		should include an explanation of how removal of the requirement will result in an "increase in efficiency of the ERO compliance program" consistent with the language of P81.
Duke Energy		Duke Energy generally supports the comments submitted by The Edison Electric Institute (EEI) and the process being used to respond to the Commission's invitation in the FFT Order.
Kansas City Power & Light		Efforts need to be made to make sure that the retirement of the requirements listed in "Proposed Requirements for Retirement in Phase 1 of Project 2013-02: Paragraph 81" don't have a ripple impact in other standards or requirements.
Entergy Services, Inc.		For future phases, indutry input should be gathered in a more formal process to allow for suggestions for re-wording or suggesting additional requirements for removal.
Tucson Electric Power		I appreciate the fact that there is a review of the NERC Standards as well as a review of the absolute need for various Standards and/or requirements. I also appreciate that the regulatory bodies are agreeable to such changes and improvements to the compliance process.
Illinois Municipal Electric Agency		Illinois Municipal Electric Agency fully supports this initiative by the collaboration group which suppports NERC's application of a risk-based focus to it's programs, and which is consistent with SPIG Recommendation 4.
Dominion		In the Complete Set of Standards with Proposed Retirements for Phase 1 pdf; Need to add IRO-001-1a R8 and MOD-004-1 R8 needs to be completely highlighted. In the Spreadsheet with Proposed Retirements; Suggest the MOD-004-1 Requirements be put in numeric order. Need to add IRO-001-1a R8; it is not listed on the spreadsheet.
South Carolina Electric and Gas		Instead of retiring R2 of EOP-009-0 could the whole standard can be replaced by the new EOP-005?

Organization	Yes or No	Question 4 Comment
Manitoba Hydro		It is not clear what will happen in instances where this project proposes to remove a requirement from a FERC approved Reliability Standard when the NERC BOT has already approved a newer version of that same standard. Will the newer BOT approved version also be modified if it includes one of the requirements in question? What if industry has already resolved one of these issues in the next version of a standard? Shouldn't we just implement the newer version?
MidAmerican Energy Company		MidAmerican Energy Company supports the draft SAR as a positive step to allow Responsible Entities, Regional Entities, NERC and FERC to focus their combined efforts on protecting the Bulk Electric System.
Idaho Power Company		MOD standards 016 through 021 should be combined into a single standard, removing duplication and retiring requirements which are "reporting-only" and/or have little discernable reliability benefit.We agree with the stated Purpose or Goal of the proposed standard of setting forth specific Reliability Standard requirement evaluation criteria and establishing a multi-phased process for addressing these Reliability Standard requirements. We agree with and support this Reliability Standard requirement evaluation and proposed multi-phased process based on the following:We believe there is value in differentiation of violations based on risk. We believe that not all violations pose the same risk to reliability, so they should not all be treated the same. Focusing on the greatest risks to reliability will allow for more efficient use of resources while improving the reliability of the BES through an application of structured risk management.
ACES Power Marketing Standards Collaborators		NERC needs to develop guidance that includes these criteria for drafting teams to avoid developing requirements that offer little reliability value in the future. There are many standards currently being developed that include similar kinds of requirements that will make a future exercise like this necessary. NERC should expend every effort to avoid such a future situation. Some examples can be found in Project 2007-09 Generator Verification. Proposed MOD-027-1 R3 through R5 largely

Organization	Yes or No	Question 4 Comment
		memorializes the administrative interactions that must occur between the GO and TP to develop a good active power/frequency control model. PRC-004-3 Part 4.2 in Project 2010-05.1 Misoperations is another example. It requires maintenance of data regarding Corrective Action Plans. These are administrative requirements and are unnecessary.
CPS Energy		No additional comments.
Independent Electricity System Operator		No comments.
Occidental Energy Ventures Corp.		OEVC Agrees with the Trade Associations on this response.
Pepco Holdings Inc & Affiliates		Pepco Holdings Inc supports this project. Additionallyl Pepco Holdings Inc supports the comments provided by EEI.
Georgia System Operations Corporation		Reliability Standard requirements are those that provide for Reliable Operation, including without limiting the foregoing, requirements for the operation of existing Facilities, including cyber security protection, and including the design of planned additions or modifications to such Facilities to the extent necessary for Reliable Operation. NERC administers other programs, such as industry alerts, reliability assessments, event and trend analyses, education, and monitoring and enforcing Reliability Standards. These other programs are designed to work in concert with Reliability Standards to support reliable operation. NERC requirements relating to administering these other programs are very important but are not Reliability Standard requirements.One of the criteria for evaluating the elimination of a Reliability Standard requirement is that it is purely reporting. There are a number of NERC requirements for these other NERC programs embedded in Reliability Standards. Most of them are purely reporting. However, to the extent that there may be other requirements for these NERC programs embedded that are not purely

Organization	Yes or No	Question 4 Comment
		reporting, they should also be considered for elimination. Reliability Standards by definition are not mechanisms for the administration of those other NERC programs.
Georgia Transmission Corporation		Reliability Standard requirements are those that provide for Reliable Operation, including without limiting the foregoing, requirements for the operation of existing Facilities, including cyber security protection, and including the design of planned additions or modifications to such Facilities to the extent necessary for Reliable Operation. NERC administers other programs, such as industry alerts, reliability assessments, event and trend analyses, education, and monitoring and enforcing Reliability Standards. These other programs are designed to work in concert with Reliability Standards to support reliable operation. NERC requirements relating to administering these other programs are very important but are not Reliability Standard requirements.One of the criteria for evaluating the elimination of a Reliability Standard requirement is that it is purely reporting. There are a number of NERC requirements for these other NERC programs embedded in Reliability Standards. Most of them are purely reporting. However, to the extent that there may be other requirements for these NERC programs embedded that are not purely reporting, they should also be considered for elimination. Reliability Standards by definition are not mechanisms for the administration of those other NERC programs. GTC recommends identifying these requirements (ex. MOD-016 through 021) and appending them to the Phase I list.
seattle city light		Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Tampa Electric Company		Tampa Electric recommends that the P81 DT ensure that the CIP requirements proposed for removal via P81 are also removed from v5 of the NERC CIP standards. Tampa Electric also supports the consideration of the following for NERC CIP standards: Removal of data collection requirements: CIP-005-3a, -4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4; R7.3CIP-008-3, -4 R2Removal of annual review requirements: CIP-002-2, -4 R4CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4

Organization	Yes or No	Question 4 Comment
		R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1
Transmission Agency of Northern California		TANC commends FERC for soliciting input on ways to eliminate requirements that are redundant or provide little protection for the bulk power system. TANC believes that NERC has proposed an appropriate response to this opportunity and looks forward to further initiatives that prioritize reliability ahead of compliance.
SERC EC Planning Standards Subcommittee		The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers.
SPP Standards Review Group		The following are typos we found in the SAR:Either delete the 'an' or make 'processes' singular in Technical Criteria B.2.(b).Either delete the 'that' in the 5th line or the 'to' in the 6th line of the Statement paragraph under CIP-001-2a R4. This is the 3rd sentence in the paragraph.Insert an 'a' between 'require' and 'new' in the last sentence of the Statement paragraph under CIP-003-3, -4 R4.2.
City of Austin dba Austin Energy		The P81 project should be considered a high priority Standards development project for the following reasons:(1) Responsive to P81 of FERC's March 15, 2012 order and SPIG Recommendation No. 4(2) Will increase efficiency of the ERO compliance programs(3) Requirements submitted for the initial phase appear to be clear candidates on their face and should not require extensive technical research(4) The collaborative nature of the project is an example for future work, because it advances the project while reducing the impact on stakeholders and NERC staff(5) The proposed pace of the project sets an example for future work (6) Furthers the focus on results, performance based Reliability Standards (7) May provide a roadmap of what should or should not be a requirement in future Reliability Standards(8) The draft P81 SAR criteria is designed to be sufficiently broad to capture all FERC approved reliability Standards that are unnecessary, redundant or do little to protect reliability (9) To eliminate Reliability Standards requirements that deter from our

Organization	Yes or No	Question 4 Comment
		focus on reliability Based on these benefits, we support the Standards Drafting Team and NERC staff working together to file the initial list of Reliability Standards for retirement with the Federal Energy Regulatory Commission prior to the end of the year and that the Standards Drafting Team also make significant progress on the scope of the phase two P81 Reliability Standards list by the end of the year.
PPL Corporation NERC Registered Affiliates		The PPL Companies generally support the concept and process being recommended, but are concerned that the stakeholder involvement in the process may be lacking. During the webinar on August 21, 2012 the drafting team members stated that the Standards Development Process will be utilized for all Phases of the project. However, the SAR does not indicate that the SDP is mandated. The Companies recommend that the entire SAR specifically state the the Standards Development Process will be used where the SDT must respond to comments and a stakeholder vote for approval. Additionally, the process should allow for individual (or groups) of stakeholders to request a standard's removal or modification that is not designated by the SDT for removal.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade		The Trade Associations believe that the P81 project should be considered a high priority Standards development project for the following reasons: o Responsive to P81 of FERC's March 15, 2012 order and SPIG Recommendation No. 4 o Will increase efficiency of the ERO compliance programs o Requirements submitted for the initial phase appear to be clear candidates on their face and should not require extensive technical research o The collaborative nature of the project is an example for future work, because it advances the project while reducing the impact on stakeholders and NERC staff o The proposed pace of the project sets an example for future work o Furthers the focus on results, performance based Reliability Standards o May provide a roadmap of what should or should not be a requirement in future Reliability Standards o The draft P81 SAR criteria are designed to be sufficiently broad to capture all FERC approved reliability Standards that are unnecessary, redundant or do little to protect reliability o Eliminating Reliability Standards requirements that are unnecessary, redundant or do little to protect reliability will

Organization	Yes or No	Question 4 Comment
Associations).		eliminate distractions from our focus on reliability Based on these benefits, the Trade Associations strongly support the Standards Drafting Team and NERC staff working together to file the initial list of Reliability Standards for retirement with the Federal Energy Regulatory Commission prior to the end of the year, and that the Standards Drafting Team also make significant progress on the scope of the phase two P81 Reliability Standards list by the end of the year.
City of Garland		This is a good start on removing requirements that are either redundant or provide little / no protection for Bulk-Power System reliability.
Electric Reliability Council of Texas, Inc.		This SAR offers significant potential value by retiring requirements that provide no BES reliability value, but nonetheless require commitment of time and resources for both regulated entities and regulators to effect and oversee compliance, respectively, and also pose liability risk for no reason, given that they provide no reliability value. However, the substance of the requirements (e.g. administrative processes, etc.) may have non-essential value unrelated to system reliability. To the extent the SDT/industry/NERC believe there may be some non-mandatory use for this information outside of the reliability standards, the information could be considered for guidance in another format, such as guidelines, best practice documentation or lessons learned. If such an effort is deemed worthwhile, it should be established in a separate process/effort, and should not distract from moving this and future phases of this SAR forward in the most efficient and effective manner to achieve the significant benefits that may result from this SAR. In addition, the standards process going forward should include consideration of whether a proposed standard addresses a reliability requirement, is cost effective and meets the reliability-based standards criteria of “what” needs to be met and not “how” an entity will meet the standard which is better address through guidelines, best practices and/or lessons learned.
Central Husdon Gas & Electric		We agree with the criteria as listed, however, we believe that another criterion must be added. This criterion is that the retirement of a requirement must not create a

Organization	Yes or No	Question 4 Comment
Corporation		compliance gap for Entities. Several of the NERC requirements have been crafted to afford Entities a means to display compliance. Retirement of these requirements can place an Entity's compliance efforts in jeopardy. A salient example of this is identified below:Central Hudson Gas & Electric Corporation strongly disagrees with the inclusion of CIP-003-3, -4 Requirements R3, R3.1, R3.2, R3.3 as candidates for retirement. The reasons stated in the SAR in favor of inclusion are that these requirements are administrative in nature and are purely examples of a documentation process. Further it is stated in the SAR that they, ".... have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements." This last statement is precisely the reason why the aforementioned requirements were included in the standard. These requirements allow Registered Entities to, on rare occasions, take an exception to one or several of the CIP requirements (for a limited period of time) if they (1) have valid cause (major emergency, Force Majeure, etc.), (2) document the occurrence and (3) are reviewed and approved by the CIP Senior Manager. This process supports the Registered Entity's compliance effort and acknowledges the need for special protocols to address emergency circumstances. Without such a process, the only recourse for the Registered Entity is to self-report a violation which is not within its control. In other words, retirement of these requirements would force the Registered Entity to be in full compliance with ALL CIP Standards ALL the time regardless of circumstance. The concept of 'realistic expectation' was undoubtedly the reason these requirements were crafted and included in the standard. Further, with regard to the Registered Entity's decision to claim an exception, a system of checks and balances already exists. At the time of a compliance audit of the standard's requirements, the Regional Entity reviews and makes a determination as to whether the actions taken by the Registered Entity were warranted.
NV Energy		We commend NERC and the Drafting Team on their efforts thus far in this important initiative. This process will serve to better focus the industry's limited resources on

Organization	Yes or No	Question 4 Comment
		activities that are necessary for reliability.
SRC		We support the P81 team's efforts and appreciate the effort to pull together this initial list of criteria and requirements. The SRC is looking forward to seeing a concrete timeline for the project.
Western Electricity Coordinating Council		WECC recognizes and appreciates the large amount of work done in a short time on this project and appreciates the opportunity to proved our comments.
American Electric Power		While AEP supports the efforts of this drafting team, it might have been advantageous to first agree on the criteria as a first phase, and then once determined, enter a second phase where requirements were proposed based upon the agreed-upon criteria. This might enable the fast-tracking of the criteria to be used by other concurrent projects and project teams.

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2013-02 Paragraph 81

The Paragraph 81 Drafting Team thanks all commenters who submitted comments on the redlined versions of 22 standards showing 38 requirements proposed to be retired. The standards were posted for a 45-day public comment period from October 25, 2012 through December 10, 2012. Stakeholders were asked to provide feedback on the standards through a special electronic comment form. There were 32 sets of comments, including comments from approximately 113 different people from approximately 64 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Ben Wu	Orange and Rockland Utilities, Inc.	NPCC	1
3.	Greg Campoli	New York Independent System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Donald Weaver	New Brunswick System Operator	NPCC	2
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Wayne Sipperly	New York Power Authority	NPCC	5
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Christina Koncz	PSEG Power LLC	NPCC	5
12.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5
15.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
16.	Robert Pellegrini	The United Illuminating Company	NPCC	1
17.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
18.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
19.	Brian Robinson	Utility Services	NPCC	8
20.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
21.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3

2.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jose Landeros	IID	WECC	1, 3, 4, 5, 6
2.	Al Juarez	IID	WECC	1, 3, 4, 5, 6
3.	Marcela Caballero	IID	WECC	1, 3, 4, 5, 6
4.	Cathy Bretz	IID	WECC	1, 3, 4, 5, 6

3.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Lee Schuster	Duke Energy	FRCC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

4.	Group	Jamison Dye	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bart McManus	Technical Operations	WECC	1
2.	Ayodele Idowu	Technical Operations	WECC	1
3.	Daniel Goodrich	Technical Operations	WECC	1
4.	Tim Loepker	Dispatch	WECC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

5.	Forrest Krigbaum	System Operations	WECC	1
6.	Huy Ngo	Design & Maint	WECC	1
7.	John Wylder	Stds Montr & Admin	WECC	1
8.	Thomas Gist	Stds Montr & Admin	WECC	1
9.	Jenny Wilson	Transmission Planning	WECC	1
10.	Larry Furumasu	Transmission Planning	WECC	1
11.	Kyle Kohne	Transmission Planning	WECC	1
12.	Richard Becker	Substation Engineering	WECC	1
13.	Kieran Connolly	Generation Scheduling	WECC	5
14.	Erika Doot	Generation Support	WECC	3, 5, 6
15.	Deanna Phillips	FERC Compliance	WECC	1, 3, 5, 6

5.	Group	Randall Heise	Dominion Resource Services	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michael	Garton	MRO	5, 6
2.	Connie	Lowe	RFC	6
3.	Louis	Slade	RFC	5
4.	Randall	Heise	NPCC	5, 6
5.	Michael	Crowley	SERC	5, 1, 3

6.	Group	Sasa Maljukan	Hydro One Networks Inc.	X									

	Additional Member	Additional Organization	Region	Segment Selection
1.	David kiguel	Hydro One Networks Inc.	NPCC	1

7.	Group	Jim Kelley	SERC EC Planning Standards Subcommittee	X				X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Sullivan	Ameren Services Company	SERC	1
2.	Charles Long	Entergy Services, Inc.	SERC	1
3.	Edin Habibovich	Entergy Services, Inc.	SERC	1
4.	James Manning	NC Electric Membership Cooperation	SERC	1
5.	Philip Kleckley	SC Electric & Gas Company	SERC	1
6.	Bob Jones	Southern Company Services	SERC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Pat Huntley	SERC Reliability Corp.	SERC 10										
8. Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 3, 5
2.	Eric Ervin	Westar Energy	SPP	1, 3, 5, 6
3.	Jonathan Hayes	Southwest Power Pool	SPP	2
4.	Bo Jones	Westar Energy	SPP	1, 3, 5, 6
5.	Tiffany Lake	Westar Energy	SPP	1, 3, 5, 6
6.	Stephen McGie	City of Coffeyville	SPP	NA
7.	Tracey Stewart	Southwestern Power Administration	SPP	1, 5
8.	Jamie Strickland	Oklahoma Gas & Electric	SPP	1, 3, 5
9.	Angela Summer	Southwestern Power Administration	SPP	1, 5

9.	Group	Jason Marshall	ACES Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bob Solomon	Hoosier Energy	RFC	1
2.	John Shaver	Arizona Electric Power Cooperative	WECC	4, 5
3.	John Shaver	Southwest Transmission Cooperative	WECC	1
4.	Amber Anderson	East Kentuck Power Cooperative	SERC	1, 3, 5
5.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT	1, 5
7.	Paul Jackson	Buckeye Power	RFC	3, 4
8.	Kevin Lyons	Central Iowa Power Cooperative	MRO	1

10.	Group	Albert DiCaprio	ISO/RTO Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Stephanie Monzon	PJM	RFC	2
2.	Bill Phillips	MISO	RFC	2
3.	Matt Goldberg	ISONE	NPCC	2
4.	Charles Yeung	SPP	SPP	2
5.	Steve Myers	ERCOT	ERCOT	2

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Greg Campoli	NYISO	NPCC 2										
7.	Ben Li	IESO	NPCC 2										
11.	Individual	Jana Van Ness, Director of Regulatory Compliance	Arizona Public Service Company	X		X		X	X				
12.	Individual	Emily Pennel	Southwest Power Pool Regional Entity										X
13.	Individual	Antonio Grayson	Southern Company	X		X		X	X				
14.	Individual	Thomas C. Duffy	Central Hudson Gas & Electric Corporation			X							
15.	Individual	David Ramkalawan	Ontario Power Generation					X					
16.	Individual	John Bee	Exelon	X		X	X	X	X				
17.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
18.	Individual	Andrew Z. Pusztai	American Transmission Company	X									
19.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
20.	Individual	David Jendras	Ameren	X		X		X	X				
21.	Individual	Patrick Brown	Essential Power, LLC					X					
22.	Individual	David Thorne	Pepco Holdings Inc.	X		X							
23.	Individual	Thad Ness	American Electric Power	X		X		X	X				
24.	Individual	Michelle D'Antuono	Occidental Energy Ventures Corp.			X		X		X			
25.	Individual	Patricia Metro	National Rural Electric Cooperative Association (NRECA)	X		X	X						
26.	Individual	Kathleen Goodman	ISO New England Inc.		X								
27.	Individual	Michael Falvo	Independent Electricity System Operator		X								
28.	Individual	Orlando Ciniglio	Idaho Power Company	X									
29.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				
30.	Individual	Jason Snodgrass	Georgia Transmission Corporation	X									
31.	Individual	Daniela Hammons	CenterPoint Energy	X									
32.	Individual	Oliver Burke	Entergy Services, Inc. (Transmission)	X									

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Summary Consideration: Thank you to Exelon and ISO New England, Inc. for supporting the comments of EEI and SRC, respectively. The Standard Drafting Team (SDT) will address the specific comments of SRC below, and notes that EEI did not submit specific comments.

Organization	Supporting Comments of "Entity Name"
Exelon	Exelon agrees with EEIs position and comments submitted related to this project.
ISO New England Inc.	ISO RTO Council Standards Review Committee (SRC)

1. If retired, do any Reliability Standard requirements proposed for retirement create a gap in reliability? If yes, please explain in the comment area.

Summary Consideration: In summary, no entity showed that a gap in reliability would result from the retirement of the proposed Reliability Standard requirements. Also, in general, the comments were very supportive of the retirement of the proposed Reliability Standard requirements, and the few questions or concerns raised are addressed in the individual responses. Based on comments and the recent approval of EOP-004-2 by the NERC Board of Trustees, CIP-001-2a R4 and EOP-004-1 R1 will be moved to Section V of the technical paper entitled: "The Initial Phase Reliability Standards Provided for Informational Purposes."

Organization	Yes or No	Question 1 Comment
ACES Standards Collaborators	No	(1) We do not see any reliability gaps created by the proposed retirements. Many of the requirements that have been moved to the second phase of the project could actually be retired in this phase without creating reliability gaps. We believe the approach to move several requirements to the second phase is overly conservative. However, we understand that drafting team must balance the retirement of requirements in this phase with satisfying concerns of stakeholders that no reliability gaps are created. (2) We are not opposed to the plan to review the linkages between BAL and INT standards in the next phase. However, we continue to believe that reloading of curtailed transactions is a commercial issue not a reliability issue. Thus, INT-004-2 easily meets criteria A and B and should be retired in phase one.
Response: ACES Standards Collaborators indicates that it did not see any reliability gaps resulting from the proposed Phase 1 retirement of requirements. The SDT acknowledges ACES Standards Collaborators' concern that deferring requirements to Phase 2 may be viewed as overly conservative, and the SDT notes that the requirements proposed in Phase 1 were influenced by the collaborative and expedited nature of Phase 1. The SDT also notes that it took just 5 months from the issuance of the Standards Authorization Request ("SAR") to a vote receiving over 90% approval for the Phase 1 requirements. In addition, on December 13, 2013, the Standards Committee passed a Reliability Standards Development Plan that requires the application of Paragraph 81		

Organization	Yes or No	Question 1 Comment
("P81") concepts to all new projects. One of the Reliability Standards Development Plan's projects is the review of the INT standards, including INT-004-2, which is scheduled to begin in the first quarter of 2013. Thus, the SDT believes that ACES Standards Collaborators' request for consideration of INT-004-2 will be timely and appropriately considered in the review of the INT standards, and, therefore, it is not necessary to include it in Phase 1 of P81.		
American Electric Power	No	AEP is not aware of any reliability gaps that would occur as a result of retiring the proposed Reliability Standards requirements.
Response: The SDT acknowledges AEP's comment that it is not aware of any reliability gaps resulting from the proposed Phase 1 retirement of requirements.		
CenterPoint Energy	No	CenterPoint Energy believes that the Reliability Standard requirements proposed for retirement in the initial phase ("Phase 1") of NERC Project 2013-02 'Paragraph 81' would not create a gap in reliability if they were retired. An increase in efficiency of the ERO compliance program should result with the removal of these Phase 1 requirements and the removal of additional Reliability Standard requirements in subsequent phases of this project.
Response: The SDT acknowledges CenterPoint Energy's comment that it believes that the proposed Phase 1 retirement of requirements should not create a gap in reliability and should also increase the efficiency of the ERO's compliance program.		
Occidental Energy Ventures Corp.	No	Occidental Energy Ventures Corp ("OEVC"). believes that the retirement of the Phase I requirements will pose little, if any, risk to the BES. However, in our view, this is a good start to a much more extensive restructuring of the regulatory model. Of course, the industry will need to gauge FERC's response to the initial grouping of requirements, but we should be prepared to aggressively push down this path.
Response: The SDT acknowledges Occidental Energy Ventures Corp's comment that it believes the proposed Phase 1 retirement of requirements will pose little, if any, risk to the Bulk Electric System, and its support for a more extensive restructuring of the regulatory model.		

Organization	Yes or No	Question 1 Comment
City of Austin dba Austin Energy	No	Please note: CIP-001-2a EA4 should be retired at the same time as CIP-001-2a R4 for the same reasons. We agree with the SDT regarding requirements applicable to the GO/GOP.
Response: During the balloting of the P81 Phase 1 requirements, EOP-004-2 was approved by stakeholders and the NERC Board of Trustees and was filed with its implementation plan on December 31, 2012 with regulatory agencies for approval. As part of the EOP-004-2 implementation plan, all of CIP-001-2a will be retired six months after regulatory approval. In the technical paper at Page 18, it was noted that: "… if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 project and may include CIP-001-2a R4 for informational purposes only." Given that a regulatory filing has been filed to retire all of CIP-001-2a, the SDT has revised the technical paper to include CIP-001-2a R4 for informational purposes only.		
Manitoba Hydro	No	Standard revision numbers and Requirement sequence changes should be made at a later date, as future revisions are required to each Standard that contains any retired Requirements. This will relieve the undesirable administrative burden, while reflecting accurate revision numbers and Requirement sequences, as changes are required to the Standards.
Response: The SDT agrees with Manitoba Hydro's comment that revisions to standard and requirement numbers should not be made at this time, given undesirable administrative burdens. The SDT has consulted with NERC staff on this issue, and no revision numbers will be implemented at this time.		
SERC EC Planning Standards Subcommittee	No	The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers"
Response: The SDT acknowledges that SERC EC Planning Standards subcommittee's comments are not the position of SERC Reliability Corporation.		

Organization	Yes or No	Question 1 Comment
Ontario Power Generation	No	The technical white paper has provided reasonable and well thought-out justifications for the retirement proposal to those reliability standard requirements.
Response: The SDT thanks Ontario Power Generation for its comment and agrees that the technical paper: "… has provided reasonable and well thought-out justifications for the retirement proposal to those reliability standard requirements."		
Southwest Power Pool Regional Entity	No	While CIP-007-3/4, Requirement R7.3 by itself has no immediate impact on the reliability of the Bulk Electric System, performance of R7.3 is required by the entity in order to be able to demonstrate compliance with CIP-007-3, Requirements R7.1 and R7.2 that, if not performed properly, could result in an impact to reliability. Elimination of this requirement could expose the registered entity to greater risk of non-compliance with the remaining requirements as it no longer requires the entity to maintain appropriate and sufficient evidence of performance with the remaining requirements. For the reasons described, the SPP RE is opposed to retiring CIP-007-3/4, Requirement R7.3.
Response: Southwest Power Pool Regional Entity states that while retirement of CIP-007-3, -4 R7.3: "… has no immediate impact on the reliability of the Bulk Electric System…" it is required to demonstrate compliance. As explained in the technical paper at Page 31, Section 400 of the NERC Rules of Procedure provides for a Regional Entity to request evidence to monitor compliance, and, therefore, it is unnecessary to also have a Reliability Standard that also requires the entity to retain records as set forth in CIP-007-3, -4 R7.3. The SDT also notes that the Responsible Entity has the burden to demonstrate compliance with CIP-007-3, -4 R7.1 and R7.2, notwithstanding the existence of CIP-007-3, -4 R7.3. For these reasons, the SDT affirms its decision to retire CIP-007-3, -4 R7.3.		
Northeast Power Coordinating Council	No	
Imperial Irrigation District (IID)	No	
Duke Energy	No	

Organization	Yes or No	Question 1 Comment
Bonneville Power Administration	No	
Dominion Resource Services	No	
Hydro One Networks Inc.	No	
SPP Standards Review Group	No	
Arizona Public Service Company	No	
Southern Company	No	
Central Hudson Gas & Electric Corporation	No	
American Transmission Company	No	
Ameren	No	
Essential Power, LLC	No	
Pepco Holdings Inc.	No	
National Rural Electric Cooperative Association (NRECA)	No	
Idaho Power Company	No	
Kansas City Power & Light	No	
Georgia Transmission Corporation	No	

Organization	Yes or No	Question 1 Comment
Entergy Services, Inc. (Transmission)	No	
Independent Electricity System Operator	Yes	1. BAL-005-0.2b, R2 - agree2. CIP-001-2a, R4 - we do not agree this is administrative in nature. Preparedness is an essential element in having the capability to readily respond to pressing reliability issues. Establishing contact with the enforcement authorities is a necessary component in preparing for reporting suspect or detected sabotage. Such reporting can help protect or minimize damages to BES facilities and/or Adverse Reliability Impact due to malicious acts. R1 to R3 do not have such a requirement to report sabotage events to the law enforcement authorities. If these authorities are included in Requirement R3, then the gap may be considered filled and R4 can be retired. However, this is not yet the case. We therefore suggest that R4 not be retired at this time.3. CIP-003-3, -4 R1.2 - agree4. CIP-003-3, -4 R3, R3.1, R3.2, R3.3 - while we agree that having the exception documented and approved by Senior Manager adds little to reliability, we do not agree that the entire requirement should be removed since this requirement is intended for implementing control of an entity's adherence to its Cyber Security policy, or document exceptions otherwise. Further, we do not concur with the SDT's view that over time, responsible entities may believe they can exempt themselves from compliance with the CIP requirements. Entities may exempt themselves from having some of their processes/procedures for cyber security not implemented, but their adherence to the policy and documenting exceptions are to be assessed during audit, which is not determined by the entities themselves. Any deviation from the requirement (the proposed "making exemption from compliance with the CIP requirement") will be identified and the entities will be found non-compliant. 5. CIP-003-3, -4 R4.2 - we agree that the action to classify the CCA information is redundant, but we do not think R4.2 can be removed entirely since the element "based on the sensitivity of the Critical Cyber Asset information" needs to be retained. Suggest to revise R4 to capture this element, or, at a minimum, consult the CIP SDT on the merit of retaining this element in R4.6. CIP-005-3a, -4a R2.6 -

Organization	Yes or No	Question 1 Comment
		agree.7. CIP-007-3, -4 R7.3 - agree.8. COM 001-1.1 R6 - agree.9. EOP-004-1 R1 - we do not agree with retiring this requirement. The RRO should have a formal reporting procedure in place to ensure adequate and detailed reporting is provided on system disturbances or any unusual event. This procedure is necessary for entities to meet the goals of further requirements in this standard that pertain to preliminary and final disturbance reporting .10. EOP-005-2 R3.1 - agree.11. EOP-009-0 R2 - agree.12. FAC-002-1 R2 - we do not agree that the requirement is burdensome. The requirement seems to meet the overarching criterion A from the White Paper (it requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES), however, at a careful reading, the requirement seems to fail meeting at least one of the Criteria B: B1 (it is administrative, but not burdensome), B2 (it is data collection/retention, but we are not sure if NERC collects this data by any other method), B3 to B6 (it does not seem to fit any of these criteria).13. FAC-008-1 R1.3.5 - agree.14. FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5 - agree.15. FAC-010-2.1 R5; FAC-011-2 R5 - agree.16. FAC-013-2 R3 - agree.17. INT-007-1 R1.2 - agree, but there needs to be a requirement somewhere to stipulate that all entities involved in the Arranged Interchange must register with NERC such that transactions' participants can be contacted for confirmation of transactions being approved or to make changes when transactions are curtailed. Until such time that this requirement is developed elsewhere, INT-007-1 R1.2 should remain in effect. 18. IRO-016-1 R2 - It does not make sense to retire this requirement, but still keep M1 - the measure associated with requirement R1 - in the standard. M1 states that each RC must have evidence, such as operator log or another data source, of actions taken for the event or disagreement or both. However, R2 is the requirement which states the RC shall document the actions taken via operator log or another data source. Therefore, removing R2 would create inconsistency in the standard.19. NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4 we agree with retiring all of the 9.1, except R9.1.2: The agreement should contain the names of the applicable entities and the responsibilities assigned to

Organization	Yes or No	Question 1 Comment
		each one in relation to the NPIR.20. PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 - agree.21. TOP-001-1a R3 - agree.22. TOP-005-2a R1 - agree.23. VAR-001-2 R5 - agree.

Response: With respect to CIP-001-2a R4, Independent Electricity System Operator (IESO) expresses a concern that without R4, entities will not be properly prepared to contact law enforcement in the event of a sabotage event. During the comment and ballot period of the P81 project, EOP-004-2 was approved by stakeholders and the NERC Board of Trustees, and was filed with its implementation plan on December 31, 2012 with regulatory agencies for approval. As part of the EOP-004-2 implementation plan, all of CIP-001-2a will be retired six months after regulatory approval. In the technical paper at Page 18, it was noted that: "… if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 Project and may include CIP-001-2a R4 for informational purposes only." Given that a regulatory filing has been filed to retire all of CIP-001-2a, the SDT has revised the technical paper to include CIP-001-2a R4 for informational purposes only. For the same reasons, in response to IESO's concern on EOP-004-1 R1, the SDT has revised the discussion of EOP-004-1 R1 to include it in the technical paper for informational purposes only.

With respect to CIP-003-3, -4 R3, IESO believes that the entire requirement should not be removed because it is a control for adhering to the Cyber Security Policy. It also states that entities do not view CIP-003-3, -4 R3 and its sub-requirements as a way to exempt themselves from compliance with the Critical Infrastructure Protection (CIP) requirements. As stated in the technical paper at page 24, an entity has the ability to implement a Cyber Security Policy that exceeds the CIP requirements without the need for CIP-003-3, -4 R3 – which could also include implementing appropriate controls. The SDT does not find that retiring CIP-003-3, -4 R3 and its sub-requirements impacts the ability of an entity to implement appropriate controls to its Cyber Security Policy. Also, as stated in the technical paper at page 24, the SDT understands that the intent of CIP-003-3-, -4 R3 and its sub-requirements has been subject to misinterpretation, notwithstanding IESO's disagreement with the SDT on this matter. Therefore, the SDT affirms that CIP-003-3, -4 R3 and its sub-requirements should be retired.

In addition, IESO believes that the language in CIP-003-3, -4, R4.2 related to: "… based on the sensitivity of the Critical Cyber Asset information …" should be retained. In the technical paper at Page 26, it was explained that this language:

". . . requires the entity to develop classifications based on a subjective understanding of sensitivity (i.e., no clear connection to serving reliability) the requirement does not support reliability. In this context, classifying based on sensitivity becomes an

Organization	Yes or No	Question 1 Comment
administrative function that becomes necessarily burdensome because of all the possible ramifications 'based on sensitivity' can produce, and, therefore, require SMEs to decide on and reduce to writing in a documented program. This is time and effort that could be better spent on other CIP activities that provide value to cyber security and actively protect the BES." IESO has not presented sufficient rationale for the SDT to reconsider its decision as explained in the technical paper. Given the rationale in the technical paper on the lack of a nexus between the language "based on the sensitivity" and reliability, the SDT affirms its decision to retire CIP-003-3, -4 R.4.2. IESO does not agree that FAC-002-1 R2 is burdensome and while it seems to meet criterion A, it believes that the requirement fails to meet at least one of the Criteria B. As stated in the technical paper on Pages 40 and 41, FAC-002-1 R2 meets Criteria B1 (administrative) and B2 (data collection/retention) because it is an administrative documentation requirement and NERC and the Regional Entities have the authority under Section 400 of the NERC Rules of Procedure to require an entity to submit data and information for purposes of monitoring compliance. This would generally occur during a spot check or compliance audit where entities would already have the obligation to produce the information required in R2 to demonstrate compliance with R1 and its sub-requirements, even without the existence of R2. Therefore, the SDT affirms that FAC-002-1 R2 should be retired. IESO further believes that INT-007-1 R1.2 may not be retired until there is another requirement requiring entities involved in Arranged Interchange to register with NERC so that participants in those transactions can contact each other when transactions are curtailed. As explained in the technical paper at Pages 56 and 57, the North American Energy Standards Board has established registry and other rules related to entities entering into Arranged Interchange, and, therefore, INT-007-1 R1.2 is no longer necessary. Therefore, the SDT affirms its decision to retire INT-007-1 R1.2. IESO states that with the retirement of IRO-016-1 R2, Measure M1 should also be retired as it relates to R2. The SDT notes that Measure M1 was not retired because it identifies how to measure compliance with IRO-016-1 R1. IESO does not agree with retiring NUC-001-2 R9.1.2, stating that "… the agreement should contain the names of the applicable entities and the responsibilities assigned to each one in relation to the NPIR." Although the SDT understands the usefulness of an agreement stating who has responsibilities for the duties set forth in the agreement, as set forth in the technical paper at Page 61, this language is contractual boilerplate and has no direct nexus to reliability. Therefore, the SDT affirms its decision to retire NUC-001-2 R9.1.2.		
Exelon	Yes	Exelon believes that if a company takes an exception it should be documented

Organization	Yes or No	Question 1 Comment
		and proposes the following revision to R3: R3. Exceptions - Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented. R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
Response: Exelon prefers a modification to CIP-003-3, -4 R3 and the sub-requirements than retirement. As explained in the technical paper at Page 26, entities have the ability to develop its own procedures to take an exemption to its Cyber Security Policy in situations that it chooses to exceed the CIP requirements without the existence of CIP-003-3, -4 R3 and the sub-requirements. Thus, an entity has the flexibility to implement the revised exemption provision after the retirement of CIP-003-3, -4 R3 and the sub-requirements. Accordingly, the SDT affirms its decision to retire the CIP-003-3, -4 R3.		
ISO/RTO Standards Review Committee		The SRC has not identified any reliability gaps caused by the proposed actions, but the SRC believes that there is value in retaining some of the deleted requirements in some other form. Documentation is not an Operating or Assessment obligation but it is a unique topic Chain-of-command should be addressed as a Certification issue or as a Assumption / Definition Issue The following requirements while not appropriate as mandatory Reliability Standards should be retained in some category (highlighted text is a proposed category)BAL-005-0.2b R2 (Current Industry Operating Practice) CIP-003-3 R1.2 CIP-003-3 R3 CIP-003-3 R4.2 CIP-003-4 R3 CIP-003-4 R3.1 CIP-003-4 R3.2CIP-003-4 R3.3 CIP-003-4 R4.2 CIP-005-3a R2.6 CIP-005-4a R2.6 CIP-007-3 R7.3 CIP-007-4 R7.3 EOP-004-1 R1 (Industry Reports)EOP-005-2 R3.1 (Annual check-up / inspection)FAC-002-1 R2 ---FAC-008-1 R2 (Chain-of-Command)FAC-008-1 R3 ---FAC-008-3 R4 (Chain-of-Command)FAC-008-3 R5 ---FAC-010-2.1 R5** (Current Industry Assessment Practice)FAC-011-2 R5** (Current Industry Assessment Practice)FAC-013-2 R3 (Business Practice - NAESB)IRO-016-1 R2 (Documentation)NUC-001-2 R9.1 (Current Industry Operating Practice)NUC-001-2 R9.1.1 (Annual check-up / inspection)NUC-001-2 R9.1.2 (Documentation)NUC-001-2 R9.1.3 (Documentation)NUC-001-2 R9.1.4

Organization	Yes or No	Question 1 Comment
		(Certification)PRC-010-0 R2 (Current Industry Assessment Practice)PRC-022-1 R2 (Documentation)Please note the IESO will submit its own comments regarding the following requirements: CIP-001-2a R4CIP-003-3 R3.1 CIP-003-3 R3.2 CIP-003-3 R3.3 CIP-003-4 R14.2INT-007-1 R1.2 (Certification)VAR-001-2 R5** (Business Practice - NAESB)

Response: The SRC states that it does not see any reliability gap with the proposed retirements; however, it provides ideas on how some requirements may be useful in another format or forum. The SDT appreciates the SRC's ideas and encourages the SRC to work with the appropriate NERC committees to discuss and possibly implement its approach.

2. Do you have any comments on the technical white paper?

Summary Consideration: A few entities provided clarifying comments for consideration in the technical white paper, and those comments have been incorporated to enhance the readability and clarity of the technical white paper. A few commenters had concerns with the discussion of specific requirements and whether this was the time to renumber requirements; these concerns are addressed in the individual comments below. There were also comments related to possible formats for Phase 2, and while not within the scope of this SDT information, was provided based on the Standard Committee's approval of the Reliability Standards Developmental Plan. A few commenters also expressed concerns that were compliance related. The SDT reminds stakeholder that the focus of the P81 effort was to retire requirements that had little or no benefit to reliability.

Organization	Yes or No	Question 2 Comment
SERC EC Planning Standards Subcommittee	No	The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers"
Response: The SDT acknowledges that SERC EC Planning Standards subcommittee's comments are not the position of SERC Reliability Corporation.		
Northeast Power Coordinating Council	No	
Imperial Irrigation District (IID)	No	
Dominion Resource Services	No	
Arizona Public Service Company	No	

Organization	Yes or No	Question 2 Comment
Ontario Power Generation	No	
Exelon	No	
American Transmission Company	No	
Ameren	No	
Essential Power, LLC	No	
American Electric Power	No	
Independent Electricity System Operator	No	
Idaho Power Company	No	
Kansas City Power & Light	No	
CenterPoint Energy	No	
Entergy Services, Inc. (Transmission)	No	
Pepco Holdings Inc.	Yes	As part of this effort, a new revision number for any standard that is changed should be used. Also any measurements or registered entities (e.g. RRO) that would no longer apply should be deleted.

Response: The SDT agrees with Pepco Holdings that measurements associated with retired requirements should be concurrently retired. The SDT points Pepco Holdings to the posted redline of the Reliability Standards that retires measurements associated with retired requirements. For administrative efficiency, the Reliability Standards will not be renumbered and functional entities will not be deleted at this time, but the next time the standard is revised it is understood that renumbering and removal of

Organization	Yes or No	Question 2 Comment
entities that are no longer applicable will occur.		
ACES Standards Collaborators	Yes	(1) On page 5, several requirements are marked with two asterisks but there is no footnote or additional information. Please indicate the purpose of the asterisks or remove them. (2) The supporting statement in the technical whitepaper and SAR that Criteria C is needed to make an informed decision "in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B" is inconsistent with the actual Criteria. Criterion C2 questions if the requirement is being reviewed in an on-going standards development project. While this is certainly a relevant question and a valid reason to not include a requirement in the P81 project, the question simply provides no input on whether Criteria A and B are met. We suggest changing the supporting statement to be clearer that Criteria C in essence is more information to make an informed decision but may not necessarily have any indication on whether Criteria A and B are satisfied. (3) The supporting statement in the technical whitepaper and SAR that Criteria C provides "additional information to assist in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B" is inconsistent with the SAR. In the detailed description, the SAR states that the initial phase shall only identify requirements that satisfy both Criteria A and B. These are supposed to be the requirements that easily meet these two criteria sets. Thus, why is Criteria C evaluated in the whitepaper. If these criteria are easily met, Criteria C is not needed to assist in the determination and the associated information while interesting would appear to be superfluous.
Response: ACES Standards Collaborators seeks clarification of the use of ** on Page 5 of the technical white paper. The SDT refers ACES Standards Collaborators to Footnote 4 of the technical white paper that states: "Those requirements that were not part of the draft SAR, but were added based on stakeholder comments are denoted by a '' throughout this technical white paper."** **ACES Standards Collaborators also seeks clarification on the role of Criteria C. The SDT notes that Criteria C was only considered after a requirement met both Criteria A and B. The application of Criteria C provided additional information that in some cases**		

Organization	Yes or No	Question 2 Comment
emphasized the need to retire the requirement (*e.g.,* was not results-based) and other times indicated that it may not be necessary to continue with retirement (*e.g.,* the requirement was already scheduled in a reasonable period of time to be retired through another standards project). The SDT believes this approach is consistent with the clarification sought by ACES Standards Collaborators, and, thus will clarify the language in the technical white paper on the application of Criteria C. The SDT also notes that the SAR states that, "…for all phases, the standard drafting team shall also consider the data and reference points set forth below in Criterion C when deciding whether a Reliability Standard requirement should be retired or modified."		
Bonneville Power Administration	Yes	BPA appreciates the drafting team's decision to include TOP-001-1 R3 in the technical white paper for informational purposes rather than proposing to retire it.
Response: The SDT is appreciative of Bonneville Power Administration's understanding of the treatment of TOP-001-1 R3.		
Central Hudson Gas & Electric Corporation	Yes	CHG&E believes the reason for retiring CIP-003-3,-4 R3 and its sub-requirements is fallacious. The reason provided in the technical white paper is essentially: " First, and most importantly, that requirement has never been available for use to exempt an entity form compliance with any requirement of any NERC reliability standard. It only applies to exceptions to internal corporate policy, and only in cases where the policy exceeds a NERC standard requirement, or addresses an issue that is not covered in a NERC reliability standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of 8 characters in length, and be changed every 30 days, this provision could be used for internal governance purposes to lessen the corporate requirement, back to the password requirements in CIP-007 R5.3, or in conjunction with a TFE to something else. The removal of this requirement has no effect on the TFE process, or compliance with any other NERC reliability standard requirement."CHG&E wishes to highlight the fact that NERC has no jurisdiction to impose or grant exceptions to internal corporate policies. Therefore, this requirement (and its sub - requirements) can only have been crafted to address exceptions to the NERC CIP requirements. Throughout this standard, the NERC requirements for a 'cyber security policy' are delineated. This requirement specifically addresses exceptions

Organization	Yes or No	Question 2 Comment
		to the 'cyber security policy'. As written, this requirement can only be interpreted to mean that an exception to the NERC CIP required 'cyber security policy' is acceptable if properly documented and approved by the CIP Senior Manager. Central Hudson Gas & Electric Corporation strongly disagrees with the inclusion of CIP-003-3, -4 Requirements R3, R3.1, R3.2, R3.3 as candidates for retirement. The reasons stated in the SAR in favor of inclusion are that these requirements are administrative in nature and are purely examples of a documentation process. Further it is stated in the SAR that they, ".... have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements." This last statement is precisely the reason why the aforementioned requirements were included in the standard. These requirements allow Registered Entities to, on rare occasions, take an exception to one or several of the CIP requirements (for a limited period of time) if they (1) have valid cause (major emergency, Force Majeure, etc.), (2) document the occurrence and (3) are reviewed and approved by the CIP Senior Manager. This process supports the Registered Entity's compliance effort and acknowledges the need for special protocols to address emergency circumstances. Without such a process, the only recourse for the Registered Entity is to self-report a violation which is not within their control. In other words, retirement of these requirements would force the Registered Entity to be in full compliance with ALL CIP Standards ALL the time regardless of circumstance. The concept of realistic expectations was undoubtedly the reason these requirements were crafted and included in the standard. Further, with regard to the Registered Entity's decision to claim an exception, a system of checks and balances already exists. At the time of a compliance audit of the standard's requirements, the Regional Entity reviews and makes a determination as to whether the actions taken by the Registered Entity were warranted. Further, the fact that this requirement is included in the FFT process is of little consolation since any exception would still constitute a violation of the NERC Standard on the part of the Registered Entity and would carry with that violation the associated stakeholder

Organization	Yes or No	Question 2 Comment
		liability.
Response: CHG&E disagrees with retiring CIP-003-3,-4 R3 and its sub-requirements. CHG&E is concerned that the language in the technical white paper on CIP-003-3,-4 R3 and its sub-requirements could be interpreted as NERC having jurisdiction to impose or grant exceptions to internal corporate policies and would require that entities be in compliance with all CIP requirements all of the time regardless of the circumstance and with no avenue to take an exemption to the CIP requirements. On the former point, the SDT clarifies that it was not the intent of the language in the technical white paper on CIP-003-3,-4 R3 and its sub-requirements to opine on the jurisdiction of NERC over "internal corporate policies." With respect to CHG&E's latter concern, it appears more compliance-related than reliability-based. The criteria set forth in the SAR and technical white paper are focused on impacts to reliability, not compliance. The SDT believes CHG&E's compliance concerns are more appropriately discussed with its Regional Entity's or NERC's compliance and enforcement monitoring staff. For informational purposes only, the SDT points to the language in CIP-003-3, -4 R1.1 "… including provision for emergency situations …" and R2.4 "The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy" as language CHG&E may wish to consider in light of its concerns." In addition, in R1 there is a requirement to "document and implement" a Cyber Security policy which at a *minimum* must contain the following: "… addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations." In discussing this with the CIP SDT leadership, it was their intent in developing this requirement to allow entities to only waive the portions of those implemented policies which were in excess of the CIP-002-3 through CIP-009-3 set of requirements. In other words, NERC and FERC would not approve this R3 requirement if it allowed waiving other requirements by simply documenting an exception. The SDT finds no reason presented by CHG&E that indicates that it should reverse its decision to retire CIP-003-3,-4 R3 and its sub-requirements. Thus, the SDT affirms its decision to retire CIP-003-3,-4 R3 and its sub-requirements.		
Manitoba Hydro	Yes	CIP-003-3,-4 R1.2: Technical Justification (page 19): CIP personnel should act based on their cyber security policy; a policy which must address the CIP-002 through CIP-009 standards as required by CIP-003 R1.1. As a result, the specific training processes and procedures will reflect the cyber security policy. We suggest "they will act via their specific training, processes and procedures which reflect the overarching cyber security policy." CIP-007-3, -4 R7.3: (1) Technical Justification (page 32): For added clarity, we suggest the wording "... small number of Reliability Standard requirements explicitly mandating ....". (2) Data and information collection for ERO compliance monitoring purposes is certainly within

Organization	Yes or No	Question 2 Comment
		the context of the Reliability Standards. For added clarity, we suggest the wording "... for ERO compliance monitoring purposes without specific data collection language in the Reliability Standards." (3) It is unclear who "the entities" are. Should this state "Responsible Entities"? (4) For additional clarity, we suggest the wording "... the Reliability Standards are arguably more difficult to understand ...".
Response: The SDT appreciates Manitoba Hydro suggested enhancements and has worked them into the technical white paper. The SDT also notes that the term Responsible Entities is defined as "entities" on Page 6 of the technical white paper.		
Southern Company	Yes	FAC-002-1 R2-The comments in the technical white paper concerning FAC-002-1 R2 are correct. Entities already have the obligation to provide the documentation of the evaluation of the reliability impact of new facilities upon request to demonstrate compliance to R1 and its sub-requirements, thus making R2 unnecessary. Furthermore, a requirement to retain documentation does not benefit or protect the reliable operation of the BES.VAR-001-2 R5: While Southern agrees that the elimination of VAR-001-2, R5 is appropriate, there is some concern that the justification that the TOP's adherence to R2 as a double check to ensure there are sufficient reactive power resources to protect the voltage levels under normal and Contingency conditions may be viewed by FERC as redirecting the burden from the PSEs and LSEs to the TOP. The LSE's (particularly) need to make their reactive resources available to the TOP in order for the TOP to acquire/use these reactive resources to protect voltage levels. Also, consider that not all entities necessarily take service under a transmission tariff, so references to other contractual mechanisms such as Interchange Agreements, etc. might be cited in the Technical White Paper for ensuring sufficient reactive resources are provided and made available by transmission customers.
Response: The SDT agrees with the clarifications suggested by Southern Company and has worked them into the technical paper.		
Georgia Transmission Corporation	Yes	GTC is very supportive of the recent ERO, Regional Entity and industry stakeholder efforts in response to the opportunity provided by FERC in paragraph 81 of the

Organization	Yes or No	Question 2 Comment
		Find, Fix, Track and Report Order to review and eliminate standards that provide no or minimal reliability benefits. However, we are disappointed with the small number of requirements that are proposed for retirement in this initial phase of work. GTC would like to note that because duplicative requirements for subsequent versions of Reliability Standards are never mandatory at the same time, the net impact of requirements being proposed for retirement identified in the "Redline of Standards with Proposed Retirements" for phase 1 is only 28 out of 1650 FERC approved requirements or 1.7%. This small percentage does not seem to reflect well on the view that NERC's FFT initiative is predicated on, of which FERC has extended an invitation to justify without imposing a deadline. From our review of the P81 Technical White Paper, it appears that there are many more requirements in addition to the 28 identified that meet the criteria for deletion. And while a phased approach has been recommended, the certainty associated with subsequent phases occurring in a timely manner is questionable and GTC recommends a big picture approach. We believe the small number of requirements identified in phase I would be more palatable if a big picture perspective was provided once submitting to FERC. For example, a breakdown similar to the one below would provide more confidence that future phases would occur and be successful: o At the end of the day, we believe we can eliminate approximately xx number or xx percentage of requirements o This will be completed in three phases o Phase one will include approximately xx requirements, posted to FERC in fourth quarter, 2012 o Phase two will include approximately xx requirements, posted to FERC in xx quarter, 2013 o Phase three posting will...Laying out the bigger picture keeps the momentum going and also let's FERC know that the first posting only begins to scratch the surface of the issue. Furthermore, we are aware of current standards drafting teams that are drafting requirements that would meet the criteria for deletion stated in this Technical White Paper. There is a pressing need to implement a mechanism to ensure "P81-qualified" requirements are not drafted going forward or eliminated prior to NERC BOT approval.GTC will continue to support this effort as it moves through the NERC standards development process and participate in future phases

Organization	Yes or No	Question 2 Comment
		of work related to the P81 project. Our goal is to ensure future phases of this effort lead to retirement of a much greater number of requirements that are not necessary for the reliability of the BES.
Response: Georgia Transmission Corporation raises points related to whether Phase 1 of P81 included sufficient requirements and the uncertainty and the timing of subsequent phases. As noted above, the Standards Committee recently approved a Reliability Standards Development Plan that requires P81 concepts to be applied to all Standard projects. Training will be offered to SDTs to ensure no new requirements would be introduced that might contradict this effort. The SDT is also encouraged that the Reliability Standards Development Plan has set forth an aggressive schedule to review the entire set of standards in 2013, many of which were identified by stakeholders in response to the draft P81 SAR.		
Hydro One Networks Inc.	Yes	Hydro One very much appreciates the efforts of the SDT in trying to streamline and focus current standards to focus on requirement that impact to reliability. In addition to this, we hope that:- Phase II of this project will continue along the same path and advance the approach to other approved standards, and- Work on new and reviewed standards will include the criteria developed in this project (i.e. SDTs are fully directed to use Paragraph 81 criteria while developing new and reviewing existing standards).
Response: As noted above, the Standards Committee recently approved a Reliability Standards Development Plan that requires P81 concepts to be applied to all standard projects. The SDT is also encouraged that the Reliability Standards Development Plan has set forth an aggressive schedule to review the entire set of standards in 2013, many of which were identified by stakeholders in response to the draft P81 SAR. Thus, the SDT is hopeful that the recent approval of the Reliability Standards Development Plan will help continue on the Phase 1 path as recommended by Hydro One Networks Inc.		
National Rural Electric Cooperative Association (NRECA)	Yes	NRECA is very supportive of the recent ERO, Regional Entities and industry stakeholder efforts in response to the opportunity provided by FERC in P81 of the Find, Fix, Track and Report Order to review and eliminate standard requirements that provide no or minimal reliability benefits. NRECA is disappointed with the small number of requirements that are proposed for retirement in this initial phase of work, but will support this effort as it moves through the NERC standards

Organization	Yes or No	Question 2 Comment
		development process and will continue participating in future phases of work related to the P81 project. It is our goal to ensure future phases of this effort lead to retirement of a much greater number of requirements that are not necessary for the reliability of the Bulk Electric System. NRECA has reviewed the P81 Technical White Paper. It appears that there are many more requirements, in addition to the 38 identified, that meet the criteria for deletion most of which were included in the SAR for this project. Although the phase approach to this project was explained and many of the requirements included in the SAR will be addressed in a subsequent phases of the project, there is a concern that the future phases of the project will not be completed in a timely manner since there is no timeline provided for the future phases in the Implementation Plan for this project. Having such a time-line will demonstrate to the FERC that the industry and the ERO are dedicated to eliminating standard requirements that provide no or minimal reliability benefits. NRECA is concerned that drafting teams are drafting requirements that would meet the criteria for deletion stated in this Technical White Paper. There must be a mechanism in place to ensure "P81-qualified" requirements are not included in standards that are under development or in standards that are provided to the NERC BOT for approval. In addition, if requirements are retired that include an entity that is only required to comply with the standard because of the specific requirement that is to be retired said entity should be removed from the applicability of the standard. An example of such is VAR-01, R5 where this requirement is the only requirement applicable to a PSE, but the PSE has not been removed from the Applicability of the standard in the red-line version posted for comment.
Response: Similar to our response to Georgia Transmission Corporation and Hydro One Networks Inc, the SDT hopes that the recent approval of the Reliability Standards Development Plan will help to alleviate any concerns of National Rural Electric Cooperative Association on the timing and content of Phase 2, as the Reliability Standards Development Plan requires P81 concepts to be applied to all standard projects. Training will also be offered to SDTs to ensure no new requirements would be introduced that might contradict this effort. The SDT also notes that the issue identified related to removing the PSE from the applicability section of VAR-001 will occur the next time that standard is reviewed and re-numbered, which based on the		

Organization	Yes or No	Question 2 Comment
Reliability Standards Developmental Plan, is scheduled for 2013.		
Occidental Energy Ventures Corp.	Yes	OEVC believes the drafting team did an excellent job researching and defending each proposed retirement. In our view, this is a fundamental necessity as we must assume that FERC will closely scrutinize each one. However, we anticipate that some form of cost/benefit analysis will be requested in each case - particularly since the entire impetus behind the Paragraph 81 project is the shortage of compliance resources. It may be a worthwhile exercise to develop a cost model that accounts for industry and CEA resources accurately and effectively. The results must be weighed against the expected benefit of any requirement - as the industry and regulatory bodies clearly have some important trade-offs to consider. In particular, with FERC's recent emphasis on cyber security, cold weather preparation, and geomagnetic protection, some of the less effective requirements need to be removed. OEVC believes that the Commission will be reluctant to proceed in this manner without data that demonstrates the comparative benefit of each requirement.
Response: Occidental Energy Ventures Corp. suggests that the SDT consider using a cost benefit analysis or exercise that accounts for industry and CEA resources. The SDT notes that the Standards Committee has approved a cost effectiveness analysis process ("CEAP") and will be implementing a pilot of this process on two standards projects in the first half of 2013. At this time, cost effectiveness considerations are not sufficiently developed to be applicable to the requirements proposed in Phase 1, nor does P81 express an expectation that such analysis for this project would be undertaken, and is focused on deletion of requirements that do little or nothing to contribute to reliability. Thus, while the SDT will not apply a cost effective test to the requirements proposed for retirement, the SDT suggests that Occidental Energy Ventures Corp. follow the developments on the CEAP Project as posted on the NERC "Standards Under Development" webpage through the Standards Committee.		
SPP Standards Review Group	Yes	Page 17 - The 6th through 12th lines are a stretch and do not add anything to the argument for retiring Requirement 3 of CIP-001-2a. It is conjecture on the part of the drafting team and should be removed from the paper. If the drafting team doesn't agree and keeps this portion, please insert the word 'require' between 'some' and 'corporate' in the 8th line. Also, delete 'to generic' in the 11th line.

Organization	Yes or No	Question 2 Comment
		Page 26 - In the 10th line of the Technical Justification paragraph, insert 'task' between 'administrative' and 'that'. Page 29 - At the beginning of the 6th line of the Technical Justification paragraph, delete the 'is'. Page 32 - In the first line of the Criterion A paragraph, insert a 'not' between 'does' and 'promote'. Page 59 - In the 8th line of the 2nd paragraph, the sentence 'Thus, IRO-016-1 R1 does not support reliability.' doesn't seem right. Shouldn't this be; it does support reliability? Or perhaps you meant to say that R2 does not support reliability. Also, in the next sentence, delete the second 'that'. Page 61 - In the 15th line of the Technical Justification paragraph, delete the 'an' in front of unnecessarily.
Response: SPP Standards Review Group suggests that the SDT remove CIP-001-2a R4 from the technical paper. As noted above, this requirement is already proposed for retirement through EOP-004-2, and, therefore, will be included in the technical paper for informational purposes only. **The SDT appreciates SPP Standards Review Group's suggestions to improve the readability of the technical paper and have made the suggested changes.**		
City of Austin dba Austin Energy	Yes	Please note: CIP-001-2a EA4 should be retired at the same time as CIP-001-2a R4 for the same reasons. We agree with the SDT regarding requirements applicable to the GO/GOP.
Response: Please see response to the City of Austin's comments to question 1.		
ISO/RTO Standards Review Committee	Yes	The SRC agrees with the removal of the identified requirements. The SRC recognizes that the scope of this SAR is to identify inappropriate requirements and not necessarily to suggest what to do with those identified requirements for removal. The SRC suggests that the Technical White Paper recognize that some of these removed requirements can and should be retained (just not retained as Reliability Standards). See response to Q1 for suggestions.

Organization	Yes or No	Question 2 Comment
Response: Please see the SDT's response to the SRC's comments to question 1.		
Southwest Power Pool Regional Entity	Yes	The white paper discussion for CIP-007-3/4, Requirement R7.3 proffers the idea that most data and information is collected for ERO compliance monitoring purposes outside of the context of Reliability Standards. While this might be the case of other standards, the SPP RE does not believe this is the case for the CIP-002 through CIP-009 Cyber Security standards, collectively referred to as the "CIP standards." The CIP standards require the entity to produce a document (e.g., policy, program, procedure, process, or list); to implement a documented program, process, or procedure; and/or to perform and document certain measurable procedural steps. In the absence of disposition records, which are specifically not required by CIP-007-3/4, Requirements R7.1 and R7.2, there will unlikely be any data or information outside of the context of the Reliability Standards demonstrating compliance with R7.1 and R7.2. The authors of the white paper appear to object to the maintenance of process documentation in this instance yet do not object to other requirements in the CIP standards that similarly call for the production and maintenance of documentation. The SPP RE is concerned that the authors of the white paper have chosen to focus on individual requirements in a stand-alone manner and have failed to understand the supportive interrelationships of the CIP standards and their requirements.
Response: Southwest Power Pool Regional Entity states that data and information related to CIP requirements are collected through the CIP requirements. Southwest Power Pool Regional Entity is particularly concerned that with the "… absence of disposition records, which are specifically not required by CIP-007-3/4, Requirements R7.1 and R7.2, there will unlikely be any data or information outside of the context of the Reliability Standards demonstrating compliance with R7.1 and R7.2." As explained above, Section 400 of the NERC Rules of Procedure provides Regional Entities with the authority to request information needed to monitor compliance and the Responsible Entity has the burden of proof to demonstrate compliance. As stated in the technical white paper at Pages 31 and 32, there is no direct nexus between data retention and reliability. This is a compliance issue that is better served through procedures promulgated outside of the Reliability Standards. Thus, the SDT affirms its decision to retire CIP-007-3, -4 R7.3.		

Organization	Yes or No	Question 2 Comment
Southwest Power Pool Regional Entity also generally questions whether the SDT understands the interrelationship between the CIP requirements, because other CIP data retention requirements are not proposed for retirement in Phase 1. The SDT notes that the number and type of CIP requirements proposed for retirement in Phase 1 was shaped to some degree by the collaborative process between stakeholders and the staffs of the Regional Entities and NERC. The SDT also collaborated with the leadership of the CIP V5 SDT on the CIP requirements proposed for retirement. The SDT's evaluations and discussions confirmed the appropriateness to retire the proposed CIP requirements. That is not to say, there are not other CIP data retention requirements that should be considered for retirement in the future. Thus, while the SDT understands Southwest Power Pool Regional Entity's concern, it affirms its decision to retire the selected CIP requirements in Phase 1.		
Duke Energy	Yes	While we agree with retiring all of the Reliability Standard requirements proposed for retirement, we believe the P81 Project Technical White Paper should be more forceful in justifying retirement of the CIP requirements. Specifically, the "not an important part of a scheme of CIP Requirements" phrase is often used in Criteria C sections discussing VFR and AML issues. It would seem that FERC may have difficulty giving this phrase credibility since (i) the industry previously had balloted to approve such requirements, (ii) NERC BOT approved such requirements, and (iii) FERC approved such requirements. All of these approvals seem to indicate that all such entities previously believed that the requirements were important to the CIP scheme. Instead, we suggest that this phrase be replaced in each instance with phrases like the following: "As explained above and since the inception of this requirement, this requirement has not been shown to constitute a [key][integral] part of a scheme of CIP requirements."
Response: The SDT appreciates Duke Energy's suggestions to clarify the technical white paper. The SDT believes that the intent of the language in the technical white paper is consistent with the suggestions of Duke Energy.		

END OF REPORT

Exhibit E

Paragraph 81 Technical Whitepaper

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Paragraph 81 Project Technical White Paper

December 20, 2012

RELIABILITY | ACCOUNTABILITY




Table of Contents

I. Introduction

On March 15, 2012, the Federal Energy Regulatory Commission ("FERC" or the "Commission") issued an order[1] on the North American Electric Reliability Corporation's ("NERC") Find, Fix and Track ("FFT") process that stated in paragraph 81 ("P81"):

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the [Electric Reliability Organization] ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

A. Consensus Process

In response to P81 and the Commission's request for comments to be coordinated,[2] during June and July 2012, various industry stakeholders, Trade

[1] *North American Electric Reliability Corporation,* 138 FERC ¶ 61,193 at P 81 (2012).

[2] In addition to addressing P81, the consensus effort was also consistent with recommendation #4 set forth in *NERC's Recommendations to Improve The Standards Development Process* at page 12 (April 2012), which states:

Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

Associations,[3] staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. Specifically, the three parties (industry stakeholders/Trade Associations, staff from NERC, and staff from the NERC Regions) used the following conservative discipline to arrive at the proposed list of requirements to be retired: (i) the development of criteria to determine whether a Reliability Standard requirement should be retired and (ii) the application of this criteria with consultation from Subject Matter Experts ("SME"), with the understanding that if any of the three parties objected to including a requirement it would not be included in the initial phase of the P81 Project. As a result of this process, a draft Standards Authorization Request ("SAR"), including an initial suggested list of requirements for retirement, was drafted and presented to the NERC Standards Committee. Also, the SMEs consulted in this process provided the technical justifications that appear in this technical white paper.

B. Standards Committee

On July 11, 2012, the Standards Committee authorized the draft SAR to be posted for industry comment and formed an interim P81 Standards Drafting Team ("SDT") to review and respond to comments as well as finalize the SAR. The draft SAR was posted on August 3, 2012 with stakeholder comments due on or before September 4, 2012. Based on the stakeholder comments received, the SDT finalized the SAR, including the criteria and the initial list of Reliability Standard requirements proposed for retirement. On September 28, 2012, the Standards Committee Executive Committee authorized: (a) waiving the 30 day initial comment period and (b) posting the SAR and list of requirements proposed for retirement in the initial phase for a 45-day formal comment period with the formation of a ballot pool during the first 30 days and an initial ballot during the last 10 days of that 45-day comment period.[4]

[3] Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, and Transmission Access Policy Study Group.

[4] The following requirements that were presented in the draft SAR were already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the Board in November), and, thus, are presented in this technical white paper in Section V for informational purposes only: CIP-001-2a R4; COM-001-1.1 R6; EOP-004-1 R1; EOP-009-0 R2; FAC-008-1 R1.3.5; PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; TOP-001-1a R3; and TOP-005-2a R1. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the Board of Trustees for retirement or filed with the Commission or Canadian governmental authorities as part of the P81 Project. Those requirements that were not part of the draft SAR, but were added based on stakeholder comments are denoted by a "**" throughout this technical white paper. More detail on each of these requirements is provided below.

P81 Project Technical White Paper

The purpose of this technical white paper is to set forth the background and technical justification for each of the Reliability Standard requirements proposed for retirement. Stakeholders are requested to review this technical white paper and provide the SDT any: (1) supplemental, additional technical justifications for a requirement(s) and/or (2) concerns with the technical justifications for a requirement(s).

II. Executive Summary

The SDT developed a set of three criteria and used them to identify requirements that could be eligible for retirement. A summary of the criteria are as follows:

A. Criterion A (Overarching Criterion): little, if any, benefit or protection to the reliable operation of the BES

B. Criteria B (Identifying Criteria)
   - B1. Administrative
   - B2. Data Collection/Data Retention
   - B3. Documentation
   - B4. Reporting
   - B5. Periodic Updates
   - B6. Commercial or Business Practice
   - B7. Redundant

C. Criteria C (Additional data and reference points)
   - C1. Part of a FFT filing
   - C2. Being reviewed in an ongoing Standards Development Project
   - C3. Violation Risk Factor ("VRF") of the requirement
   - C4. Tier in the 2013 Actively Monitored List ("AML")
   - C5. Negative impact on NERC's reliability principles
   - C6. Negative impact on the defense in depth protection of the BES
   - C7. Promotion of results or performance based Reliability Standards

Specifically, for a requirement to be proposed for retirement, it must satisfy both, Criterion A and at least one of the Criteria B. Criteria C were considered as additional information to make a more informed decision.

Based on the criteria above, the SDT proposes to retire the following 36 requirements in 23 Reliability Standard versions:

- BAL-005-0.2b R2
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3

- CIP-003-3 R4.2
- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2
- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-1 R2
- FAC-008-1 R3
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5**
- FAC-011-2 R5**
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5**

A table is included in Appendix A with the Reliability Standard requirements proposed for retirement and a cross-reference to the associated criteria.

III. Criteria

The P81 Project focuses on identifying FERC-approved Reliability Standard requirements that satisfy the criteria set forth below.[5] Specifically, for a Reliability

[5] The scope of future phases of the P81 Project has not yet been determined. When the scope is considered, the criteria set forth herein may be a useful guide to appropriate criteria for those phases.

Standard requirement to be proposed for retirement it must satisfy **both**: (i) Criterion A (the overarching criterion) and (ii) at least one of the Criteria B listed below (identifying criteria). The purpose of having these two levels of criteria was to confine the review and consideration of requirements to only those requirements that clearly need not be included in the mandatory Reliability Standards. Also, Criteria A and B were designed so there would be no rewriting or consolidation of requirements, and the technical merits of retiring the requirements did not require significant research and vetting. In addition, for each Reliability Standard requirement proposed for retirement, the data and reference points set forth below in Criteria C were considered to make a more informed decision on whether to proceed with retirement. Lastly, for each requirement proposed for retirement, any increase to the efficiency of the ERO compliance program is addressed.

Criterion A (Overarching Criterion)

The Reliability Standard requirement requires responsible entities ("entities") to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Section 215(a) (4) of the United States Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

Criteria B (Identifying Criteria)

B1. Administrative

The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

This criterion is designed to identify requirements that can be removed with little effect on reliability and whose removal will result in an increase in the efficiency of the ERO compliance program. Administrative functions may include a task that is or is not related to developing procedures or plans, such as establishing communication contacts. Thus, for certain requirements, Criterion B1 is closely related to Criteria B2, B3 and B4. Strictly administrative functions do not inherently negatively impact reliability directly and, where possible, should be eliminated for purposes of efficiency and to allow the ERO and entities to appropriately allocate resources.

B2. Data Collection/Data Retention

These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

This criterion is designed to identify requirements that can be removed with little effect on reliability. The collection and/or retention of data do not necessarily have a reliability benefit and yet are often required to demonstrate compliance. Where data collection and/or data retention is unnecessary for reliability purposes, such requirements should be eliminated in order to increase the efficiency of the ERO compliance program.

B3. Documentation

The Reliability Standard requirement requires responsible entities to develop a document (*e.g.,* plan, policy or procedure) which is not necessary to protect BES reliability.

This criterion is designed to identify requirements that require the development of a document that is unrelated to reliability or has no performance or results-based function. In other words, the document is required, but no execution of a reliability activity or task is associated with or required by the document.

B4. Reporting

The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there would be little reliability impact.

B5. Periodic Updates

The Reliability Standard requirement requires responsible entities to periodically update (*e.g.,* annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

This criterion is designed to identify requirements that impose an updating requirement that is out of sync with the actual operations of the BES, unnecessary or duplicative.

B6. Commercial or Business Practice

The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

This criterion is designed to identify those requirements that require: (i) implementing a best or outdated business practice or (ii) implicating the exchange of or debate on commercially sensitive information while doing little, if anything, to promote the reliable operation of the BES.

B7. Redundant

The Reliability Standard requirement is redundant with: (i) another FERC-approved Reliability Standard requirement(s); (ii) the ERO compliance and monitoring program or (iii) a governmental regulation (*e.g.*, Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

This criterion is designed to identify requirements that are redundant with other requirements and are, therefore, unnecessary. Unlike the other criteria listed in Criterion B, in the case of redundancy, the task or activity itself may contribute to a reliable BES, but it is not necessary to have two duplicative requirements on the same or similar task or activity. Such requirements can be removed with little or no effect on reliability and removal will result in an increase in efficiency of the ERO compliance program.

Criteria C (Additional data and reference points)

To assist in the determination of whether to proceed with the retirement of a Reliability Standard requirement that satisfies both Criteria A and B, the following data and reference points shall be considered to make a more informed decision:

C1. Was the Reliability Standard requirement part of a FFT filing?

The application of this criterion involves determining whether the requirement was included in a FFT filing.

C2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?

The application of this criterion involves determining whether the requirement proposed for retirement is part of an active on-going Standards Development Project, with a consideration of the point in the process that Project is at. If the requirement has been passed by the stakeholders and is scheduled to be presented to the NERC Board of Trustees, in most cases it will not be included in the P81 project to promote regulatory efficiency. The exception would be a requirement, such as the Critical Information Protection ("CIP") requirements for Version 3 and 4, that is not due to be retired for an extended period of time; or, other requirements that based on the specific facts and circumstances of that requirement indicate it should be retired via the P81 Project first rather than waiting for another Standards Development Project to retire it, particularly as a way to increase the efficiencies of the ERO compliance program. Also, for informational purposes, whether the requirement is included in a future or pending Standards Development Project will be identified and discussed.

C3. What is the VRF of the Reliability Standard requirement?

The application of this criterion involves identifying the VRF of the requirement proposed for retirement, with particular consideration of any requirement that has been assigned as having a Medium or High VRF. Also, the fact that a requirement has a Lower VRF is not dispositive that it qualifies for retirement. In this regard, Criterion C3 is considered in light of Criterion C5 (Reliability Principles) and C6 (Defense in Depth)

to ensure that no reliability gap would be created by the retirement of the Lower VRF requirement. For example, no requirement, including a Lower VRF requirement, should be retired if its retirement harms the effectiveness of a larger scheme of requirements that are purposely designed to protect the reliable operation of the BES.

C4. In which tier of the 2013 AML does the Reliability Standard requirement fall?

The application of this criterion involves identifying whether the requirement proposed for retirement is on the 2013 AML, with particular consideration for any requirement in the first tier of the 2013 AML.

C5. Is there a possible negative impact on NERC's published and posted reliability principles?

The application of this criterion involves consideration of the eight following reliability principles published on the NERC webpage.

> **Reliability Principles**
> NERC Reliability Standards are based on certain reliability principles that define the foundation of reliability for North American bulk power systems. Each reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of reliability of the North American bulk power systems. Each reliability standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.
>
> Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
>
> Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
>
> Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

Principle 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

Principle 7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks. (footnote omitted).

C6. Is there any negative impact on the defense in depth protection of the BES?

The application of this criterion considers whether the requirement proposed for retirement is part of a defense in depth protection strategy. In order words, the assessment is to verify whether other requirements rely on the requirement proposed for retirement to protect the BES.

C7. Does the retirement promote results or performance based Reliability Standards?

The application of this criterion considers whether the requirement, if retired, will promote the initiative to implement results- and/or performance-based Reliability Standards.

IV. The Initial Phase Reliability Standards Requirements Proposed for Retirement

The following lists the requirements proposed for retirement with details of the assessment resulting from the applicability of the criteria above.

BAL-005-0.2b R2 – Automatic Generation Control

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

Background/Commission Directives

BAL-005-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[6] Also, the Commission accepted an errata filing to BAL-005-0.1b, which replaced Appendix 1 with a corrected version of a Commission-approved interpretation, and made an internal reference correction in the interpretation, thus resulting in BAL-005-0.2b.[7]

In Order No. 693 at paragraph 387, the Commission stated that:

> The goal of this Reliability Standard is to maintain Interconnection frequency by requiring that all generation, transmission, and customer load be within the metered boundaries of a balancing authority area, and establishing the functional requirements for the balancing authority's regulation service, including its calculation of ACE.

At paragraph 396, the Commission stated:

> On this issue, the Commission directs the ERO to modify BAL-005-0 through the Reliability Standards development process to develop a process to calculate the minimum regulating reserve for a balancing authority, taking into account expected load and generation variation and transactions being ramped into or out of the balancing authority.

This Commission directive is unaffected by the proposed retirement of BAL-005-0.2b R2.

Additionally, when adjusting the VRF for the previous version, BAL-005-0.1b R2, from Lower to High, the Commission stated that:[8]

> While theoretically, CPS can be met without the use of AGC, for example, when the AGC system is malfunctioning, the Commission believes, in practice, that AGC is the most dependable and effective means for multiple balancing authorities in an Interconnection to collectively meet CPS requirements in tandem while minimizing assistance from each other in this regard. Human reaction is neither fast enough nor dependable

[6] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[7] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Errata Changes to Seven Reliability Standards, Docket No. RD12-4-000 (September 13, 2012).

[8] *North American Electric Reliability Corporation*, 121 FERC ¶ 61,179 at P 50 (2007).

> enough in this repetitive task to provide the immediate and continuous support to correct for Interconnection frequency drift. Further, the failure to use AGC presents a higher risk that immediate load shedding will need to be implemented after the sudden loss of generation or an unforeseen significant load increase and, thus, the failure to use AGC subjects the Bulk-Power System to a higher risk of instability.

However, the fact that the VRF for BAL-005-0.2b R2 is High is not indicative of its actual impact on the BES as explained in further detail below. Also, no Commission directive is impacted by BAL-005-0.2b R2.

Technical Justification

The stated reliability purpose of BAL-005-0.2b is to establish requirements for Balancing Authority Automatic Generation Control ("AGC") necessary to calculate Area Control Error ("ACE") and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved. The reliability purpose and objectives of BAL-005-0.2b are unaffected by the proposed retirement of R2.

A Balancing Authority must use AGC to control its Regulating Reserves to meet the Control Performance Standards ("CPS") as set forth in BAL-001-0.1a R1 and R2. Although for a short period of time (as the Commission stated during an AGC malfunction) a Balancing Authority may be able to meet its CPS obligations without AGC, it cannot do so for any extended period of time, and, therefore, Balancing Authorities must use AGC to control its Regulating Reserves to satisfy its obligations under BAL-001-0.1a R1 and R2. Given this fact, it is redundant to also have BAL-005-0.2b R2 set forth the following statement: "Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard." (Criterion B7). It is the duplicative nature of having two requirements requiring the same activity that does little, if anything, to benefit or protect reliable operation of the BES. (Criterion A). In other words, without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a R1 and R2.

Also, the retirement of BAL-005-0.2b R2 would increase the efficiency of the ERO compliance program because NERC and the Regional Entities would be able to focus their time and resources on monitoring compliance on BAL-001-0.1a R1 and R2, which are results-based requirements, versus monitoring compliance with both BAL-001-0.1a R1 and R2 as well as the static statement in BAL-005-0.2b R2. Therefore, retiring BAL-005-0.2b R2 will provide for increased efficiencies in the ERO compliance program.

Criterion A

Without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a

R1 and R2. Having two requirements requiring a Balancing Authority to conduct the same activity or task does little, if anything, to benefit or protect the reliable operation of the BES because it is duplicative.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. BAL-005-0.2b R2 has not been part of a FFT filing.

2. BAL-005-0.2b R2 is currently scheduled to be included in Standards Development Project 2010-14.2, which is Phase II of Balancing Authority Reliability-based Controls: Time Error, AGC, and Inadvertent. Given that Project 2010-14.2 is currently not an active Standards Development Project, it remains appropriate to retire BAL-005-0.2b R2 via the P81 Project.

3. The VRF for BAL-005-0.2b R2 is High. Given the redundant nature of BAL-005-0.2b R2, the High VRF is not dispositive of whether or not it should be retired since BAL-001-0.1a R1 and R2 accomplishes the important reliability requirement of Balancing Authorities maintaining Regulating Reserves that can be controlled by AGC to satisfy CPS.

4. BAL-005-0.2b R2 is not part of the 2013 AML.

5. The redundant nature of BAL-005-0.2b R2 with BAL-001-0.1a R1 and R2 also indicates that the retirement of BAL-005-0.2b R2 does not pose a negative impact to NERC's published and posted reliability principles. The two reliability principles applicable to BAL-005-0.2b R2 are the following:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement of BAL-005-0.2b R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. As discussed above, given that BAL-001-0.1a R1 and R2 already require that AGC be used to control Regulating Reserves, there is no risk or gap to reliability resulting from the retirement of BAL-005-0.2b R2.

7. Retirement of BAL-005-0.2b R2 promotes a results-based approach, because it is retiring a static requirement while BAL-001-0.1a R1 and R2, which are more dynamic and results-based requirements, will remain in effect.

Accordingly, for the above reasons, it is appropriate to retire BAL-005-0.2b R2.

CIP-003-3, -4 R1.2 – Cyber Security – Security Management Controls

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[9] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[10] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[11] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[12]

In Order No. 706 at paragraph 342 the Commission stated that:

> Reliability Standard CIP-003-1 seeks to ensure that each responsible entity has minimum security management controls in place to protect the critical cyber assets identified pursuant to CIP-002-1. To achieve this goal, a responsible entity must develop a cyber security policy that represents management's commitment and ability to secure its critical cyber assets. It also must designate a senior manager to direct the cyber security program and to approve any exception to the policy.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R1.2 does not impact a Commission directive.

Technical Justification

[9] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).
[10] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards).
[11] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[12] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

The importance of the cyber security policy as representing management's commitment and ability to secure critical cyber assets is overshadowed by the rigorous and specific training, procedural and process related requirements of the CIP Standards. These trainings, procedures and processes render having the cyber security policy readily available an unnecessary requirement. In other words, whether CIP personnel are completing a typical CIP requirement cyber security task or responding to an immediate situation, they will act via their specific training, processes and procedures and not the overarching cyber security policy. Stated another way, CIP personnel will act via their specific training, processes and procedures which reflect the overarching cyber security policy. Consequently, the cyber security policy's generalized guidance on compliance with the CIP requirements is not a document that adds value to personnel protecting the BES from a cyber attack on a day-to-day basis.

Furthermore, to implement CIP-003-3, -4 R1.2 entities have undertaken a variety of administrative solutions including kiosks dedicated to computers with the cyber security policy, posting the policy on the company intranet, having copies available in work stations, at common area desks in generating stations and substations, etc. Therefore, although the cyber security policy is readily available for all personnel who have access to, or are responsible for, Critical Cyber Assets, these personnel are specifically and appropriately focused on implementing the procedures and processes required by CIP Reliability Standards such as CIP-007-3 R1, which states as follows:

> Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

Generally the cyber security policy will cite CIP-007-3 R1 as a requirement, and may refer to procedures related to CIP-007-3 R1, but will not have, nor is it required to have, the detail necessary to implement CIP-007-3 R1. In some larger companies, it is also common to have specific procedures on how to accomplish requirements such as CIP-007-3 R1 in a control center versus a generating plant or substation, and it may be different CIP personnel implementing these procedures in locations many hundreds of miles, states or Interconnections away from each other. The value of a more general cyber security policy to these individuals is minimal, at best, and, therefore, does not support reliability. Also, making it readily available at all office locations is an unnecessarily burdensome administrative task.

Moreover, to place every procedure and process to comply with CIP in the cyber security policy is also not practical or effective, because such a large policy will only distract from CIP personnel being able to specifically focus on the task before them. As already stated,

there are likely some differences between implementing a requirement like CIP-007-1 R1 in a control center that may be located in one state and for generators located several states and hundreds of miles away. Thus, making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES (Criteria A and B1).

In this context, also consider the inefficiencies CIP-003-3, -4 R1.2 may be causing the ERO compliance program. In companies with hundreds of personnel who have access to, or are responsible for, Critical Cyber Assets in multiple states and Interconnections, the ERO may expend a significant amount of time and resources to monitor compliance with CIP-003-3, -4 R1.2 via a review of kiosks, intranet sites, office cubicles, desks, etc in multiple locations. Accordingly, considerable efficiency gains will be obtained for the ERO's compliance program if CIP-003-3, -4 R1.2 is retired.

Criterion A
Making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. CIP-003-3, -4 R1.2 has been part of a FFT filing.[13]

2. As is the case with all the CIP requirements (other than CIP-001-2a R4) proposed for retirement in this technical paper, CIP-003-3, -4 R1.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security) ("CIP V5"). The P81 SDT has coordinated its efforts with the chair of Project 2008-06. There is no conflict between CIP requirements proposed in this technical white paper for retirement and the direction of Project 2008-06. The CIP V5 requirements are not Board of Trustee or Commission approved, and, even if they were, the effective date of CIP V5 is unknown and likely at least a year, maybe more, into the future. Thus, unlike the other requirements presented here for informational purposes, it is appropriate to maintain all the CIP requirements discussed in this technical paper within the scope of the P81 Project to secure the efficiency gains resulting to the ERO compliance program from their retirement.

3. CIP-003-3, -4 R1.2 has a Lower VRF. As explained above, CIP-003-3, -4 R1.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

[13] NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

4. CIP-003-3,-4 R1.2 is in the second tier of the AML. As explained above, CIP-003-3, -4 R1.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given its administrative nature, CIP-003-3, -4 R1.2 does not negatively impact NERC's published and posted reliability principles. The two reliability principles that appear applicable to CIP-003-3, -4 R1.2 are the following:

   Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

   Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks.

   As stated above, other CIP requirements are replete with the requirements that CIP personnel implement to protect the BES from cyber attacks.

6. Retiring CIP-003-3, -4 R1.2 does not negatively impact defense in depth because no other requirement depends on the cyber security policy being readily available. Therefore, the removal of CIP-003-3,-4 R1.2 cannot have a negative impact on defense in depth.

7. Retirement of CIP-003-3, -4 R1.2 promotes a results-based approach because the requirement is mechanistic and administrative, and does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R1.2.

CIP-003-3, -4 R3, R3.1, R3.2, R3.3 – Cyber Security – Security Management Controls

R3. Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[14] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[15] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[16] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[17]

In Order No. 706 at paragraphs 373 and 376 the Commission stated that:

> Requirement R3 provides that a responsible entity must document exceptions to its policy with documentation and senior management approval. The Commission is concerned that, if exceptions mount, there would come a point where the exceptions rather than the rule prevail. In such a situation, it is questionable whether the responsible entity is actually implementing a security policy. We therefore believe that the Regional Entities should perform an oversight role in providing accountability of a responsible entity that excepts itself from compliance with the provisions of its cyber security policy. Further, we believe that such oversight would impose a limited additional burden on a responsible entity because Requirement R3 currently requires documentation of exceptions.
>
> Further, the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this

[14] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).
[15] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[16] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[17] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

> clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 do not impact a Commission directive.

Technical Justification

CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 (CIP exception requirements) have proven not to be useful and have been subject to misinterpretation. For instance, although the CIP exception requirements have not been available for use to exempt an entity from compliance with any requirement of any Reliability Standard, based on questions received by NERC CIP Staff, entities may be interpreting the CIP exception requirements to allow for such an exemption. The CIP exception requirements only apply to exceptions to internal corporate policy, and only in cases where the policy exceeds a Reliability Standard requirement or addresses an issue that is not covered in a Reliability Standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of eight characters in length, and be changed every 30 days, which is over and above what is required in CIP-007-3 R5.3, the CIP exception requirements could be invoked for internal governance purposes to lessen the corporate requirement back to the password requirements in CIP-007-3 R5.3, but under no circumstances do the CIP exception requirements authorize the implementation of security measures less than what is required in CIP-007-3 R5.3.

The retirement of the CIP exception requirements would not impact an entity's ability to maintain such an exception process within their corporate policy governance procedures, if it so desired. Consequently, the CIP exception requirements were always an internal administrative and documentation requirement that is outside the scope of the other CIP requirements (Criteria B1 and B3). In this context, the CIP exception requirements do not support the level of reliability set forth in the Reliability Standards, and are unnecessarily burdensome because they have resulted in entities implementing practices due to a misinterpretation of the requirement that has caused them to allocate time and resources to tasks that are misaligned with the requirements themselves. Unfortunately, this misunderstanding has also impacted the efficiency of the ERO compliance program because of the amount of time and resources needed to clear up the misunderstanding and coach entities on the meaning of the CIP exception requirements. These inefficiencies would be eliminated with the retirement of the CIP exception requirements. Accordingly, as explained, the CIP exception requirements are an administrative tool for internal corporate governance procedures, and, therefore, are not requirements that are necessary or directly protect the BES from a cyber attack, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A).

Criterion A
The CIP exception requirements are a tool for internal corporate governance procedures and is not a requirement directly protecting the BES from a cyber attack, and, therefore, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C
1. The CIP exception requirements have been part of a FFT filing.[18]

2. The CIP exception requirements are part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between the CIP exception requirements proposed in this technical white paper for retirement and the direction of Project 2008-06.

3. The CIP exception requirements each have a Lower VRF. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. The CIP exception requirements are on the third tier of the AML. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the administrative and unnecessary nature of the CIP exception requirements in relation to protecting the BES from cyber attacks, retirement does not pose any negative impact to NERC's published and posted reliability principles, of which only Principle 8 appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. Retiring the CIP exception requirements does not negatively impact any defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of the CIP exception requirements promotes a results-based approach because the CIP exception requirements are approaches that entities may voluntarily take to handle internal corporate governance procedures, and, therefore, do not provide the foundation for performing a required reliability task.

[18] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-6-000 (December 30, 2011).

Accordingly, for the above reasons, it is appropriate to retire the following CIP exception requirements: CIP-003-3, -4 R3, R3.1, R3.2, and R3.3.

CIP-003-3, -4 R4.2 - Cyber Security – Security Management Controls

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Background/Commission Directives
CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[19] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[20] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[21] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[22] In Order No. 706, the Commission did not specifically address CIP-003-3, -4 R4.2.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R4.2 does not impact a Commission directive.

Technical Justification
The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an unnecessarily administrative and a documentation task that is redundant with CIP-003-3, -4 R4 (Criteria A, B1, B3 and B7). Specifically, CIP-003-3, -4 R4[23] already requires the classification of information associated with Critical Cyber Assets. The only difference between R4 and R4.2 is that the subjective term "based on the sensitivity" has been added, thus, making it essentially redundant. Further, CIP-003-3, -4 R4 requires the entity to develop classifications based on a subjective understanding of sensitivity (*i.e.*, no clear connection to serving reliability), the requirement does not support reliability. In this context, classifying based on sensitivity becomes an administrative task that becomes necessarily burdensome, because of all the possible ramifications "based on sensitivity" can produce, and, therefore, require SMEs to decide on and reduce to writing in a documented

[19] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[20] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[21] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[22] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, (2012).
[23] "**R4**. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets."

program. This is time and effort that could be better spent on other CIP activities that provide value to cyber security and actively protect the BES. For similar reasons, retiring CIP-003-3, -4 R4.2 and the term "based on sensitivity" would increase the efficiencies of the ERO compliance program on several levels. The ERO would not spend time and resources on reviewing whether an entity's documentation contained classifications "based on sensitivity," and, instead would be able to focus its time and resources monitoring compliance with the entity's program to identify, classify, and protect information associated with Critical Cyber Assets (R4), without any distraction on monitoring the subjective implementation of classifications based on sensitivity (R4.2).

Criterion A
The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an administrative and a documentation task that is redundant with CIP-003-3, -4 R4.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)
- Criterion B7 (Redundant)

Criteria C

1. CIP-003-3, -4 R4.2 has been part of a FFT filing.[24]

2. CIP-003-3, -4 R4.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-003-3, -4 R4.2 and the direction of Project 2008-06.

3. CIP-003-3, -4 R4.2 has a Lower VRF. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-003-3, -4 R4.2 is on the third tier of the AML. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the unnecessary and redundant nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8 which appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

[24] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

6. Retirement of CIP-003-3, -4 R4.2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of CIP-003-3, -4 R4.2 promotes a results-based approach because retiring CIP-003-3, -4 R4.2 moves away from prescriptive, checklist of documentation approach to Reliability Standard requirements.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R4.2.

CIP-005-3a, -4a R2.6 – Cyber Security – Electronic Security Perimeter(s)

R2.6. Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

Background/Commission Directives

CIP-005-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[25] CIP-005-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RD09-7-000 and RM06-22-000 and was approved on September 30, 2009.[26] CIP-005-2a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by unpublished letter order on February 2, 2011.[27] CIP-005-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[28] CIP-005-3a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by an unpublished letter order on February 2, 2011.[29] CIP-005-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No. 761.[30] CIP-005-4a was filed for Commission approval as errata to the CIP Version 4 Petition on April 12,

[25] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[26] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[27] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).
[28] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[29] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).
[30] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No 761, the Final Rule on the CIP Version 4 standards.[31]

In Order 706 at paragraph 505 the Commission noted that:

> Requirement R2 of CIP-005-1 requires a responsible entity to implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-005-3, -4 R2.6 does not impact a Commission directive.

Technical Justification

The implementation of an appropriate use banner ("banner") on a user's screen for all interactive access attempts into the Electronic Security Perimeter ("ESP") is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES. Specifically, the banner does not support reliability because people who intend to inappropriately use sites will simply ignore the banner. (Criterion A). The banner is also an administrative task since it simply requires a message be displayed on an access screen. Furthermore, the implementation and administration of a non-beneficial tool, such as the banner, therefore creates a needlessly burdensome task. As mentioned, above, the ineffectiveness of the banner also indicates that it does not support reliability. (Criteria B1 and B3). In addition, banners of this type are generally considered to be a form of legal protection or mitigation of liability, rather than security protection. Furthermore, the banner does not ensure a proper or secure access point configuration which is generally the purpose of CIP-005-3a, -4a. Further, this requirement has also been the subject of numerous TFEs for devices that cannot support such a banner, and hence has diverted resources from more productive efforts. Thus, the ERO's compliance program would become more efficient if CIP-005-3a, -4a R2.6 was retired, because ERO time and resources could be reallocated to monitor compliance with the remainder of CIP-005-3a, -4a, which provides for more effective controls of electronic access at all electronic access points into the ESP.

Criterion A

The implementation of an appropriate use banner on a user's screen for all interactive access attempts into the ESP is an activity or task that does little, if anything, to benefit or protect reliable operation of the BES, because it is administrative and a static electronic message that is not an effective deterrent or control against unauthorized access.

[31] *Id.*

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C

1. CIP-005-3a, -4a R2.6 has been part of a FFT filing.[32]

2. CIP-005-3a, -4a R2.6 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-005-3a, -4a R2.6 and the direction of Project 2008-06.

3. The VRF for CIP-005-3a, -4a R2.6 is Lower. As explained above, CIP-005-3a, -4a R2.6 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-005-3a, -4a R2.6 is on the first tier of the AML; however, given its clear ineffective nature the placement on the first tier is not dispositive of whether it should be retired.

5. Reliability principle No. 8 – "Bulk power systems shall be protected from malicious physical or cyber attacks" – is not implicated or negatively impacted by the retirement of CIP-005-3a, -4a R2.6, because it is not an effective deterrent or control to unauthorized access into an ESP.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. Furthermore, the remainder of CIP-005-3a, -4a provides for actual controls of electronic access at all electronic access points which addresses the reliability risk associated with unauthorized access into an ESP.

7. Its retirement also promotes a results-based approach because CIP-005-3a, -4a R2.6 is an ineffective administrative task, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-005-3a, -4a R2.6.

CIP-007-3, -4 R7.3 – Cyber Security – Systems Security Management

[32] NERC FFT Informational Filing, Docket No. RC12-13-000 (June 29, 2012); NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012).

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Background/Commission Directives

CIP-007-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[33] CIP-007-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[34] CIP-007-2a was filed for Commission approval on November 17, 2009 in Docket No. RD10-3-000 and was approved on March 18, 2010.[35] CIP-007-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[36] CIP-007-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[37]

In Order No. 706 at paragraph 631 the Commission stated that:

> Requirement R7 of CIP-007-1 requires the responsible entity to establish formal methods, processes and procedures for disposal or redeployment of cyber assets. In the CIP NOPR, the Commission addressed the concern that solely to "erase the data," as stated several times in Requirement R7, may not be adequate because technology exists that allows retrieval of "erased" data from storage devices, and that effective protection requires discarded or redeployed assets to undergo high quality degaussing. We noted that erasure is as much a method as it is a goal, and that the requirement ultimately needs to assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. Degaussing is not the sole means for achieving this goal. The Commission therefore proposed to direct the ERO to modify Requirement R7 to clarify this point. (Footnote omitted)

This Commission directive is unaffected by the retirement of CIP-007-3,-4 R7.3 as explained below.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to

[33] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[34] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[35] Order Approving Reliability Standard Interpretation, 130 FERC ¶ 61,184 (2010).
[36] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[37] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

submit data and information for purposes of monitoring compliance. [38] CIP-007-3, -4 R7.3 requires the maintaining of records for the purpose of demonstrating compliance with disposing of or redeploying of Cyber Assets in accordance with documented procedures. NERC and the Regions Entities, however, under Section 400 already have the ability to require the production of records to demonstrate compliance, thus it is unnecessary to also state the same in CIP-007-3, -4 R7.3. The maintaining of records is an administrative task, not a task directly related to the protection of the BES from a cyber attack. The maintaining of records is not a task that by itself, or in conjunction with other requirements, supports reliability. Also, the maintaining of the records becomes unnecessarily burdensome in that it requires all records be maintained, which may or may not be necessary to demonstrate compliance via the production of information under Section 400. (Criteria B1 and B2). As mentioned, CIP-007-3, -4 R7.3 does not promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A).

In contrast, the remaining substantive requirements in R7 read as follows:

> R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.
>
> R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
>
> R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

An entity's following of these requirements may help to protect BES reliability, but the retention of evidence associated with these requirements does not. Hypothetically, an entity could perform R7, R7.1 and R7.2 flawlessly and protect the BES, but not have any record of it. While this situation may impact a demonstration of compliance, the lack of

[38] Section 401 of NERC's Rules of Procedure provide for collection of data and information necessary to monitor compliance outside the context of Reliability Standards:

> **Data Access** — All Bulk Power System owners, operators, and users shall provide to NERC and the applicable Regional Entity such information as is necessary to monitor compliance with the Reliability Standards. NERC and the applicable Regional Entity will define the data retention and reporting requirements in the Reliability Standards *and compliance reporting procedures.* (emphasis added).

records does not necessarily directly impact the reliability of the BES or protect it from a cyber attack.

Also, there are some inherent inefficiencies resulting from a small number of Reliability Standard requirements explicitly mandating the collection of data, evidence and records, while most data and information is collected for ERO compliance monitoring purposes without specific data collection language in the Reliability Standards. In this regard, for the ERO, Regional Entities and the entities, Reliability Standards are arguably more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A
CIP-007-3, -4 R7.3 does not promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. CIP-007-3, -4 R7.3 has not been part of a FFT filing.

2. CIP-007-3, -4 R7.3 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-007-3, -4 R7.3 and the direction of Project 2008-06.

3. The VRF for CIP-007-3, -4 R7.3 is Lower. As explained above, CIP-007-3, -4 R7.3 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-007-3, -4 R7.3 is on the first tier of the AML; however, given that it is simply requiring the retention of records the fact that is on the first tier is not dispositive of whether it should be retired.

5. Given the administrative, data collection nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. The retirement does not negatively impact defense in depth because data retention in-and-of-itself is not an activity that other requirements depend on to help cover a reliability gap or risk to reliability.

7. Its retirement promotes a results-based approach because the data collection/retention does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-007-3, -4 R7.3.

EOP-005-2 R3.1– System Restoration from Blackstart Resources

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

Background/Commission Directives
EOP-005-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[39] EOP-005-2 was submitted for Commission approval on December 31, 2009 in Docket No. RM10-16-000 and was approved on March 17, 2011 in Order No. 749.[40] Although the Commission did not address EOP-005-2 R3 directly in Order No. 749, it stated at paragraph 17 the following:

> EOP-005-2 and EOP-006-2 clarify the responsibilities of the reliability coordinator and transmission operator in the restoration process and restoration planning and address the Commission's directives in Order No. 693 related to the EOP Standards. By enhancing the rigor of the restoration planning process, the Reliability Standards represent an improvement from the current Standards and will improve the reliability of the Bulk-Power System. The Commission is not directing any modifications to the three new Reliability Standards. Nevertheless, as discussed below, commenters raised several issues for consideration, at the time these standards are next revisited, which we believe could improve these new Reliability Standards

[39] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 (2007).
[40] *System Restoration Reliability Standards*, 134 FERC ¶ 61,215, (March 17, 2011) ("Order No. 749"), *order on clarification*, 136 FERC ¶ 61,030 ("Order No. 749-A") (2011).

There are no outstanding Commission directives that are affected by the proposed retirement of EOP-005-2 R3.1.

Technical Justification

The reliability purpose of EOP-005-2 is to ensure that plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure that reliability is maintained during restoration and priority is placed on restoring the Interconnection. This reliability purpose is unaffected by the proposed retirement of R3.1.

A review of EOP-005-2 R3.1 indicates that this requirement is redundant with EOP-005-2 R3 and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1, B5 and B7). The primary reason EOP-005-2 R3.1 is unnecessary is that EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes. EOP-005-2 R3 reads:

> Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule.

Consequently, since R3 requires the Transmission Operator to submit its restoration plan to the Reliability Coordinator whether or not there has been a change, R3.1 only adds a separate, duplicative administrative burden for the entity to also confirm that there were no changes based upon another pre-determined schedule. While R3.1 may have attempted to capture the likelihood that unless there have been significant changes to the entity's BES, there would be no change to the restoration plan, this is an insufficient reason to impose a needlessly burdensome, duplicative administrative requirement relative to the language in R3. EOP-005-2 R3.1 is also clearly needlessly burdensome if one considers that the time and resources of Transmission Operators is better spent reliably operating the BES, rather than submitting paperwork to a Reliability Coordinator on possibly two different pre-determined schedules – one for changes and one for no changes. For these reasons, there is no reliability gap resulting from the retirement of EOP-005-2 R3.1 because Transmission Operators already have an obligation to review and provide its restoration plan annually on a mutually agreed predetermined schedule to its Reliability Coordinator. It could also be argued that a reason for both R3 and R3.1 is for the Reliability Coordinator to organize the Transmission Operator submittals into changes versus no changes. However, with the requirement to annually review restoration plans comes the need to demonstrate and track annual reviews via the revision history index, for example, which quickly shows the Reliability Coordinator when changes have and have not occurred.

The retirement of EOP-005-2 R3.1 would also increase the efficiencies of the ERO compliance program because the ERO would be able to focus its time and resources on R3 which already captures R3.1 and not be concerned with tracking the submission of

restoration plans on multiple pre-determined schedules, some with changes and some without changes. Instead, the focus of the ERO compliance program would be on whether the Transmission Operators annually submitted its restoration plan to its Reliability Coordinator on one pre-determined schedule. Thus, the retirement of EOP-005-2 R3.1 appears to benefit the ERO compliance program.

Criterion A
EOP-005-2 R3.1 is redundant and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)
- Criterion B5 (Periodic Updates)
- Criterion B7 (Redundant)

Criteria C
1. EOP-005-2 R3.1 has not been part of a FFT filing.

2. EOP-005-2 R3.1 is not part of an on-going Standards Development Project.

3. EOP-005-2 R3.1 does not yet have a FERC-approved VRF.

4. EOP-005-2 R3.1 is on the second tier of the AML; however, the duplicative nature of R3 and R3.1 discounts any indication that R3.1 being in the second tier is a reason not to proceed with its retirement.

5. Since EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes, retirement of EOP-005-2 R3.1 does not pose any negative impact to the following of NERC's published and posted reliability principles that appear to apply:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

6. Retirement of EOP-005-2 R3.1 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of EOP-005-2 R3.1 promotes a results-based approach because the requirement is administrative and unnecessary, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire EOP-005-2 R3.1.

FAC-002-1 R2 – Coordination of Plans for New Facilities

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

Background/Commission Directives
FAC-002-0 was submitted to the Commission for approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[41] FAC-002-1 was submitted for Commission approval on September 9, 2010 in Docket No. RD10-15-000 and was approved on January 10, 2011.[42] When approving FAC-002-0 in Order No. 693 at paragraphs 692 and 693, and FAC-002-1 in a subsequent order,[43] the Commission did not directly address R2.

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-002-1 R2.

Technical Justification
Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, without the existence of FAC-002-1 R2, a Regional Entity or NERC has the ability to request and receive "documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems)." This generally would occur during a spot check or compliance audit where entities have the obligation to

[41] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[42] NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2 RD10-15-000 (January 10, 2011).
[43] *North American Electric Reliability Corporation*, 134 FERC ¶ 61,015 (2011).

provide documentation sufficient to demonstrate compliance. In this regard, entities already have the obligation to produce the same information required in R2 to demonstrate compliance to R1 and its sub-requirements, thus making R2 unnecessary. To have a Reliability Standard requirement that is setting forth a data retention requirement and a requirement for the entity to deliver, upon request, that data to NERC or a Regional Entity is unnecessary and also repetitive with the NERC Rules of Procedure. Accordingly, retiring FAC-002-1 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. Thus, FAC-002-1 R2 is not necessary to support reliability. Consequently, a review of R2 indicates that it is an administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). The compilation of three years of data is a burdensome task, particularly when one considers the resources and time spent on stockpiling this information is better spent coordinating the studies, executing an interconnection agreement and ensuring that interconnections are safely and reliably energized, maintained and operated. Also, there are some inherent inefficiencies that result from a small number of requirements, such as CIP-007-3, -4 R7.3 and FAC-002-1 R2 being data, evidence and record retention requirements, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A

A review of FAC-002-1 R2 indicates that it is an administrative and data collection requirement that does little, if anything, to benefit or protect reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. FAC-002-1 R2 has not been part of a FFT filing.

2. FAC-002-1 R2 is subject to a future Project 2010-02 Connecting New Facilities to the Grid (a review of FAC-001 and FAC-002) that is scheduled to begin in the second quarter of 2015. It seems appropriate to retire FAC-002-1 R2 at this time as it may also make the review of FAC-001 and FAC-002 more effective and efficient.

3. FAC-002-1 R2 has a Lower VRF.

4. FAC-002-1 R2 is in the third tier of the AML.

5. The retirement of FAC-002-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since there are no directly applicable reliability principles.

6. The retirement does not negatively impact defense in depth because the compilation of studies for three years has no operational or planning relationship with any other requirement.

7. The retirement of FAC-002-1 R2 promotes a results-based approach since the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-002-1 R2.

FAC-008-1 R2; FAC-008-1 R3;[44] - Facility Ratings Methodology

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

Background/Commission Directives
FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[45]

[44] Unlike the other requirements presented for informational purposes only, FAC-008-1 R2 and FAC-008-1 R3 have been maintained within the scope of P81 given that they are essentially identical to FAC-008-3 R4 and FAC-008-3 R5. Inclusion would also appear to be consistent with increasing ERO compliance program efficiencies. FAC-008-1 R2 and FAC-008-1 R3 became inactive on December 31, 2012, due to FAC-008-3 becoming enforceable on January 1, 2013.

[45] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-1 R2 and R3.

Technical Justification

FAC-008-1 R2 and R3 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-1 R2 and R3 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-1 regarding their facility rating methodologies whether or not the exchange envisioned by FAC-008-1 R2 and R3 occurs. Furthermore, neither FAC-008-1 R2 and R3 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-1 R2 and R3 are designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its generator step up ("GSU") transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, operating conditions, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of System Operating Limits ("SOLs"), Interconnection Reliability Operating Limits ("IROLs"), calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments).[46] Accordingly, the requirements in FAC-008-1 R2 and FAC-008-1 R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect

[46] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-02 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element.

the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange of comments and compliance with the substantive requirements of FAC-008-1. Instead of spending time and resources on FAC-008-1 R2 and R3, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-1.

Criterion A
The requirements in FAC-008-1 R2 and R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-008-1 R2 and R3 have not been part of a FFT filing.

2. FAC-008-1 R2 and R3 are not subject to an on-going Standards Development Project.

3. FAC-008-1 R2 and R3 have a Lower VRF.

4. FAC-008-1 R2 and R3 are in the third tier of the AML.

5. The retirement of FAC-008-1 R2 and R3 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-008-1 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-1 R2 and R3, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These requirements may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-1 R2 and R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-1 R2 and R3.

FAC-008-3 R4; FAC-008-3 R5 – Facility Ratings

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.

Background/Commission Directives
FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[47] "On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No.

[47] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[48] FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[49]

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-3 R4 and R5.

Technical Justification

FAC-008-3 R4 and R5 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-3 R4 and R5 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-3 regarding their facility rating methodologies whether or not the exchange envisioned by FAC-008-3 R4 and R5 occurs. Further, neither FAC-008-3 R4 nor R5 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-3 R4 and R5 are designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its GSU transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, historical performance, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of SOLs, IROLs, calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments).[50] Accordingly, the

[48] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[49] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).
[50] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-2 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0,

requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-008-3. Instead of spending time and resources on FAC-008-3 R4 and R5, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-3. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-3.

Criterion A
The requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-008-3 R4 and R5 have not been part of a FFT filing.

2. FAC-008-3 R4 and R5 are not subject to an on-going Standards Development Project.

3. FAC-008-3 R4 and R5 have a Lower VRF.

4. FAC-008-3 R4 and R5 are in the third tier of the AML.

5. The retirement of FAC-008-3 R4 and R5 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under

---

footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element. Also, FAC-008-3 R7 and R8 require the transmission of facility ratings to reliability entities.

normal and abnormal conditions as defined in the NERC Standards.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-008-3 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-3 R4 and R5, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-3 R4 and R5 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-3 R4 and R5.

***FAC-010-2.1 R5 – System Operating Limits Methodology for the Planning Horizon*

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives

FAC-010-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[51] FAC-010-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[52] FAC-010-2.1 was filed for Commission approval on November 20, 2009 in Docket No. RD10-9-000

[51] *Facilities Design, Connections and Maintenance Reliability Standards,* 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).

[52] *Version Two Facilities Design, Connections and Maintenance Reliability Standards,* 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).

and was approved on April 19, 2010.[53] In Order No. 722,[54] the Commission approved FAC-010-2.1 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

Technical Justification
The reliability purpose of FAC-010-2.1, to ensure that System Operating Limits used in the reliable planning of the BES are determined based on an established methodology, is unaffected by the proposed retirement of R5. FAC-010-2.1 R5 requires that when a Planning Authority receives comments on its SOL methodology, it must respond and indicate whether it has changed its methodology. The retirement of FAC-010-2.1 R5 does not create a reliability gap, because the Planning Authority must comply with the substantive requirements of FAC-010-2.1 whether or not the exchange envisioned by FAC-010-2.1 R5 occurs. FAC-010-2.1 R5 may support an avenue to advance commercial interests.

For example, if a Transmission Operator or Transmission Planner is also a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Planning Authority's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of its development of a facility ratings methodology under FAC-008-1, -3 than the Planning Authority's methodology. FAC-010-2.1 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Planning Authority's SOL methodology. Accordingly, FAC-010-2.1 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-010-2.1. Instead of spending time and resources on FAC-010-2.1, a Planning Authority's time and resources would be better spent complying with the substantive requirements of FAC-010-2.1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Planning Authority's adherence to substantive requirements of FAC-010-2.1.

Criterion A
The requirement in FAC-010-2.1 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

[53] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Transmission Operations Reliability Standards, Docket No. RD10-9-000 (April 19, 2010).
[54] *Version Two Facilities Design, Connections and Maintenance Reliability Standards* 125 FERC ¶ 61,040 (2009).

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-010-2.1 R5 has not been part of a FFT filing.

2. FAC-010-2.1 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011. Thus, it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-010-2.1 R5 has a Lower VRF.

4. FAC-010-2.1 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-010-2.1 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-010-2.1 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-010-2.1 R5.

***FAC-011-2 R5– System Operating Limits Methodology for the Operations Horizon*

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives
FAC-011-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[55] FAC-011-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[56] In Order No. 722, the Commission approved FAC-011-2 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

Technical Justification
FAC-011-2 R5 requires that when a Reliability Coordinator receives comments on its SOL methodology that it must respond and indicate whether it has changed its methodology. The retirement of FAC-011-2 R5 does not create a reliability gap, because the Reliability Coordinator must comply with the substantive requirements of FAC-011-2 R5 whether or not the exchange envisioned by FAC-011-2 R5 occurs. FAC-011-2 R5 may support an avenue to advance commercial interests.

For example, similar to FAC-010-2.1 R5, if a Transmission Operator or Transmission Planner also is a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Reliability Coordinator's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of the development of its facility ratings methodology under FAC-008-1, -3 than the Reliability Coordinator's methodology. FAC-011-2 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Reliability Coordinator's SOL methodology. Accordingly, FAC-011-2 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the

[55] *Facilities Design, Connections and Maintenance Reliability Standards,* 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).
[56] *Version Two Facilities Design, Connections and Maintenance Reliability Standards,* 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).

potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-011-2. Instead of spending time and resources on FAC-011-2 R5 a Reliability Coordinator's time and resources would be better spent complying with the substantive requirements of FAC-011-2 R5. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-011-2 R5.

Criterion A
The requirement in FAC-011-2 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-011-2 R5 has not been part of a FFT filing.

2. FAC-011-2 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011which is not currently scheduled and thus it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-011-2 R5 has a Lower VRF.

4. FAC-011-2 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available

> to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-011-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-011-2 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-011-2 R5.

FAC-013-2 R3 – Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.

Background/Commission Directives

FAC-013-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[57] FAC-013-2 was submitted for Commission approval on January 28, 2011 in Docket No. RD11-3-000 and was approved on November 17, 2011.[58]

In Order No. 729, the Commission denied NERC's request to withdraw FAC-012-1 and retire FAC-013-1, and directed as follows at paragraph 291:

> 291. The Commission hereby adopts its NOPR proposal to deny NERC's request to withdraw FAC-012-1 and retire FAC-013-1. Instead, pursuant to section 215(d)(5) of the FPA and section 39.5(f) of our regulations, the Commission directs the ERO to develop modifications to FAC-012-1 and FAC-013-1 to

[57] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[58] *Order Approving Reliability Standard*, 137 FERC ¶ 61,131 (2011).

> comply with the relevant directives of Order No. 693 and, as otherwise necessary, to make the requirements of those Reliability Standards consistent with those of the MOD Reliability Standards approved herein as well as this Final Rule. These modifications should also remove redundant provisions for the calculation of transfer capability addressed elsewhere in the MOD Reliability Standards. In making these revisions, the ERO should consider the development of a methodology for calculation of inter-regional and intra-regional transfer capabilities. The Commission accepts the ERO's request for additional time to prepare the modifications and so directs the ERO to submit the modifications to FAC-012-1 and FAC-013-1 no later than 60 days before the MOD Reliability Standards become effective.

Although the Commission did not directly address the merits of FAC-013-2 R3 when approving FAC-013-2,[59] similar to FAC-008-3, the developer of the Transfer Capability methodology and data must follow specific technical requirements and provide the data to reliability entities for use in their models. There are no outstanding Commission directives with respect to this R3.

Technical Justification

A review of FAC-013-2 R3 indicates that it is a needlessly burdensome administrative task that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B4). Specifically, FAC-013-2 R1 and its sub-requirements set forth the information that each Planning Authority must include when developing its Transfer Capability methodology. FAC-013-2 R3 sets forth a requirement that if an entity comments on this methodology, the Planning Authority must respond and indicate whether or not it will make a change to its Transfer Capability methodology. Thus, while R1 sets forth substantive requirements, R3 sets forth more of an administrative task of the Planning Authority responding to comments on its methodology.

The following NERC glossary definition of Transfer Capability states:

> The measure of the ability of interconnected electric systems to move or transfer power *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is *not g*enerally equal to the transfer capability from "Area B" to "Area A."

In the context of a Planning Authority engaging in an exchange with an entity over the Transfer Capability there is a possibility of a scenario that a group of generators[60] try to

[59] *Id.* (approval of FAC-013-2).

[60] Generators that receive the Transfer Capability methodology via an association with one of the entities in the R2 sub-requirements.

get the Planning Authority to revise its Transfer Capability methodology to advance commercial interests via changes to the methodology that would increase or decrease transfer capability from Area A to Area B. (Criterion B6). Such issues should be raised in the context of receipt of transmission services, not the Reliability Standards. Moreover, even without the possible commercial motivation of certain entities to get the Planning Authority to revise its Transfer Capability methodology, implementing an exchange between entities and the Planning Authority seems much better suited via regional planning committees, than mandatory Reliability Standards.

In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-013-2. Instead of spending time and resources on FAC-013-2 R3, time and resources would be better spent complying with the substantive requirements of FAC-013-2. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-013-2.

Criterion A
The requirement in FAC-013-2 R3 to respond to comments on the Transfer Capability methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-013-2 R3 has not been part of a FFT filing.

2. FAC-013-2 R3 is not subject to an on-going Standards Development Project.

3. FAC-013-2 R3 has a Lower VRF.

4. FAC-013-2 R3 is not on the AML.

5. The retirement of FAC-013-2 R3 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-013-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of FAC-013-2 R3 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-013-2 R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-013-2 R3.

INT-007-1 R1.2 – Interchange Confirmation

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

Background/Commission Directives
INT-007-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[61] The Commission did not directly address INT-007-1 R1.2 when it approved the Reliability Standard in Order No. 693 at paragraph 867.

There are no outstanding Commission directives with respect to R1.2.

Technical Justification
The reliability purpose of INT-007-1 is to ensure that each Arranged Interchange is checked for reliability before it is implemented. The reliability purpose of INT-007-1 is unaffected by the proposed retirement of R1.2.

INT-007-1 R1.2 is a needlessly burdensome administrative task that does not support reliability because it is now outdated. (Criterion B1). At one time the identification

[61] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

number came from the NERC TSIN system, by now it is handled via NAESB Electric Industry Registry.[62] Also, under the E-Tag protocols, no entity may engage in an Interchange transaction without first registering with the E-Tag system and receiving an identification number. Further, the entity desiring the transaction enters this identification number in the E-Tag system to pre-qualify and engage in an Arranged Interchange. Accordingly, the task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A). The ERO compliance program would benefit and be more efficient if it was not monitoring an outdated requirement.

Criterion A
The task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. INT-007-1 R1.2 has not been part of a FFT filing.

2. INT-007-1 R1.2 is part of a pending Standards Development Project – Project 2008-12 Coordinate Interchange Standards, which is estimated to start in the second quarter of 2013. Given this timeline, it is appropriate to move forward with the retirement of INT-007-1 R1.2. Such a retirement may also help to streamline Project 2008-12 once it is active and progressing.

3. INT-007-1 R1.2 has a Lower VRF.

4. INT-007-1 R1.2 is not on the AML.

5. The retirement of INT-007-1 R1.2 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

    Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

    Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

[62] *See, North American Energy Standards Board Webregistry Technical Guide v1.4* (Proprietary) (July 2012). The new NAESB system has updated and implemented more automation to the process.

It is the adherence to the substantive requirements of INT-007-1 that promotes these posted reliability principles, not R1.2.

6. The retirement of INT-007-1 R1.2 does not impact any defense in depth strategies because the task is no longer necessary.

7. The retirement of INT-007-1 R1.2 promotes a results-based approach because the requirement does not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire INT-007-1 R1.2.

IRO-016-1 R2 – Coordination of Real-time Activities Between Reliability Coordinators

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

Background/Commission Directives
IRO-016-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693. The Commission did not directly address R2 when approving IRO-016-1 in Order No. 693 at paragraphs 1004 and 1005. There are no outstanding Commission directives with respect to R2.

Technical Justification
The reliability purpose of IRO-016-1 is to ensure that each Reliability Coordinator's operations are coordinated such that they will not have an adverse reliability impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations. To implement the purpose, IRO-016-1 R1 and its sub-requirements state:

> **R1.** The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
>
> **R1.1.** If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.

> **R1.2.** If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
>
> **R1.2.1.** If time permits, this re-evaluation shall be done before taking corrective actions.
>
> **R1.2.2.** If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

These requirements are specific actions and decision points among Reliability Coordinators that promote the reliable operation of the BES. In contrast, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Therefore, the reliability purpose of IRO-016-1 is unaffected by the proposed retirement of R2.

Furthermore, outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, the retirement of IRO-016-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to demonstrate compliance with IRO-016-1 R1 and its sub-requirements. Accordingly, retiring IRO-016-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. Thus, IRO-016-1 R2 does not support reliability. Consequently, R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as IRO-016-1 R2 being a data, evidence and record retention requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A
A review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. IRO-016-1 R2 has not been part of a FFT filing

2. IRO-016-1 R2 is not subject to an on-going Standards Development project.

3. IRO-016-1 R2 has a Lower VRF.

4. IRO-016-1 R2 is not on the AML.

5. The retirement of IRO-016-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since none of the principles appear to apply to a data retention requirement.

6. IRO-016-1 R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of IRO-016-1 R2 promotes a results-based approach because the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire IRO-016-1 R2.

NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4 – Nuclear Plant Interface Coordination

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement.

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3. A requirement to review the agreement(s) at least every three years.

R9.1.4. A dispute resolution mechanism.

Background/Commission Directives

NUC-001-1 was submitted for Commission approval on November 19, 2007 in Docket No. RM08-3-000 and was approved on October 16, 2008.[63] NUC-001-2 was submitted for Commission approval on August 14, 2009 in Docket No. RD09-10-000 and was approved on January 21, 2010.[64]

Although in Order No. 716 the merits of R9.1 and its sub-requirements were not directly addressed, the Commission did state the following in the context of the VRFs for all of R9:[65]

> Consistent with the NOPR, the Commission directs the ERO to revise the violation risk factor assignment for Requirement R9 from lower to medium. The Commission disagrees with commenters that a lower violation risk factor is appropriate because Requirement R9 is an administrative requirement to include the specified provisions. While the Commission recognized in the NOPR that many of the requirements of the proposed Reliability Standard are administrative in nature, these same requirements provide for the development of procedures to ensure the safe and reliable operation of the grid, and responses to potential emergency conditions.

There are no outstanding Commission directives with respect to these requirements.

Technical Justification

The reliability purpose of NUC-001-2 is to ensure the coordination between Nuclear Plant Generator Operators and Transmission Entities for nuclear plant safe operation and shutdown. The reliability purpose of NUC-001-2 is unaffected by the proposed retirement of requirements 9.1, 9.1.1, 9.1.2, 9.1.3 and 9.1.4. Requirement 9.1 and its sub-requirements specify certain administrative elements that must be included in the agreement (required by R2) between the Nuclear Plant Generator Operator and the applicable Transmission Entities. These are a mix of technical, communication, training and administrative requirements. Of those that may be classified as administrative, R9.1 and its sub-requirements clearly stand out as unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A and B1). R9.1 and its sub-requirements are a check list of certain non-technical boilerplate provisions generally included in modern agreements. These provisions do not directly relate to protecting BES reliability. Further, requiring via a mandatory Reliability Standard the inclusion of boilerplate provisions is unnecessarily burdensome relative to the other significant requirements in NUC-001-2 that pertain to performance based reliability coordination and protocols between Transmission Entities

[63] *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008) ("Order No. 716"), *order on reh'g*, Order No. 716-A, 126 FERC ¶ 61,122 (2009).
[64] *Order Approving Reliability Standard*, 130 FERC ¶ 61,051 (2010).
[65] NUC-001-1 was approved in Order No. 716, while NUC-001-2 was approved without discussion of R9.1 and its sub-requirements in a subsequent order. *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008); 130 FERC ¶ 61,051 (2010).

and Nuclear Plant Generator Operators. Therefore, the retirement of NUC-001-2 R9.1 and all its sub-requirements creates no reliability gap and are the type of provisions that would likely be in a modern agreement anyway.

For these same reasons, the ERO compliance program efficiency will increase with the retirement of NUC-001-2 R9.1 and its sub-requirements because compliance monitoring time and resources will not be spent conducting a checklist of whether an agreement includes boilerplate provisions, and instead, the time and resources may be spent reviewing adherence with the technical, substantive coordination and protocol provisions of NUC-001-2.

Criterion A
R9.1 and its sub-requirements are unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)

Criteria C
1. NUC-001-2 R9.1 and its sub-requirements have not been part of a FFT filing.

2. NUC-001-2 R9.1 and its sub-requirements are not part of an on-going Standards Development Project, but NUC-001-2 is part of Project 2012-13, which is a placeholder for a five year review. Given the as yet undetermined start date for Project 2012-13, it is appropriate to move forward with the retirement of NUC-001-2 R9.1 and its sub-requirements.

3. Individual VRFs are not assigned to the sub-requirements of NUC-001-2 R9.

4. NUC-001-2 R9.1 and its sub-requirements are in the third tier of the AML.

5. The retirement of NUC-001-2 R9.1 and its sub-requirements do not pose any negative impact to NERC's published and posted reliability principles, since none of them seem to apply to the inclusion of boilerplate contractual provisions.

6. There is no impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of NUC-001-2 R9.1 and its sub-requirements promote a results-based approach by eliminating administrative check-list requirements.

Accordingly, for the above reasons, it is appropriate to retire NUC-001-2 R9.1 and its sub-requirements.

PRC-010-0 R2 – Assessment of the Design and Effectiveness of UVLS Program;

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

Background/Commission Directives

PRC-010-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[66] Although not specifically addressing PRC-010-0 R2, in Order No. 693 at paragraph 1506 and 1507 the Commission stated that:

> With regard to ISO-NE's disagreement on integration of various system protections "because such integration cannot be technologically accomplished", we note that the evidence collected in the Blackout Report indicates that "the relay protection settings for the transmission lines, generators and underfrequency load shedding in the northeast may not be entirely appropriate and are certainly not coordinated and integrated to reduce the likelihood and consequence of a cascade – nor were they intended to do so." In addition, the Blackout Report stated that one of the common causes of major outages in North America is a lack of coordination on system protection. The Commission agrees with the protection experts who participated in the investigation, formulated Blackout Recommendation No. 21 and recommended that UVLS programs have an integrated approach.
>
> Regarding FirstEnergy's question of whether universal coordination among UVLS programs that address local system problems makes sense, we believe that PRC-010-0's objective in requiring an integrated and coordinated approach is to address the possible adverse interactions of these protection systems among themselves and to determine whether they could aggravate or accelerate cascading events. We do not believe this Reliability Standard is aimed at universal coordination among UVLS programs that address local system problems. (Footnote omitted).

The retirement of PRC-010-0 R2 does not affect a Commission directive.

Technical Justification

[66] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its current UVLS program assessment for purposes of monitoring compliance. Thus, the retirement of PRC-010-0 R2 does not affect the ability of NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-010-0 R1 and its sub-requirements. Furthermore, PRC-010-0 R1 requires that the entity document an assessment of the effectiveness of its UVLS program:

> The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program.

Accordingly, retiring PRC-010-0 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. A review of R2 indicates that it is a needlessly burdensome administrative and data collection/retention requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as PRC-010-0 R2 being a data production requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401.

Criterion A
R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C
1. PRC-010-0 R2 has not been part of a FFT filing.

2. PRC-010-0 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-010-0 R2 in the P81 Project.

3. This requirement has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-010-0 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-010-0 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-010-0 R2.

PRC-022-1 R2 – Under-Voltage Load Shedding Program Performance

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

Background/Commission Directives
PRC-022-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[67] In Order No. 693 at paragraph 1565 the Commission approved PRC-022-1 without a discussion of R2. There are no outstanding Commission directives with respect to R2.

Technical Justification
Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its analysis of UVLS program performance for purposes of monitoring compliance. Thus, the retirement of PRC-022-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-022-1 R1 and its sub-requirements. Furthermore, PRC-022-1 R1 already requires that the entity document UVLS performance:

> Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage

[67] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations.

Accordingly, retiring PRC-022-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. In this context, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, similar to the retention of records requirements in CIP-007-3, -4 R7.3, FAC-002-1 R2 and PRC-010-0 R2, the ERO compliance program efficiency will increase since it will no longer need to track a static requirement of whether a UVLS program assessment was submitted within 30 days of a request by NERC or the Regional Entity, and instead, compliance monitoring may focus on the more substantive requirements of PRC-022-1.

Criterion A
R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C
1. PRC-022-1 R2 has not been part of a FFT filing.

2. PRC-022-1 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-022-1 R2 in the P81 Project.

3. PRC-022-1 R2 has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-022-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-022-1 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-022-1 R2.

***VAR-001-2 R5 – Voltage and Reactive Control*

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

Background/Commission Directives
VAR-001-1 was submitted for Commission approval on April 4, 2006, in Docket No. RM06-16-000. When approving VAR-001-1, in Order No. 693 at paragraph 1858,[68] the Commission recognized:

> . . . that all transmission customers of public utilities are required to purchase Ancillary Service No. 2 under the OATT or self-supply, but the OATT does not require them to provide information to transmission operators needed to accurately study reactive power needs. The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities.

On September 9, 2010, NERC submitted VAR-001-2, which included revisions to Requirement R5 to satisfy Commission directives in Order No. 693, including the directive in paragraph 1858. This directive was addressed by adding "Load Serving Entities" to the standard as applicable entities and making them subject to the same requirements as Purchasing Selling Entities. These modifications to VAR-001-2 were accepted by the Commission on January 10, 2011.[69]

Technical Justification
VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* open access transmission tariff ("OATT"). (Criteria A and B7). To elaborate, VAR-001-2 R5 provides for the PSE and LSE (transmission customers) to arrange for or self provide reactive resources the same as required under Schedule 2 of the OATT. Specifically, as a general matter Schedule 2 of the OATT states:

[68] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[69] *North American Electric Reliability Corp.*, 134 FERC ¶ 61,015 (2011).

Schedule 2 Reactive Supply and Voltage Control from Generation or Other

In order to maintain transmission voltages on the Transmission Provider's transmission facilities within acceptable limits, generation facilities and non-generation resources capable of providing this service that are under the control of the control area operator) are operated to produce (or absorb) reactive power. Thus, Reactive Supply and Voltage Control from Generation or Other Sources Service must be provided for each transaction on the Transmission Provider's transmission facilities. The amount of Reactive Supply and Voltage Control from Generation or Other Sources Service that must be supplied with respect to the Transmission Customer's transaction will be determined based on the reactive power support necessary to maintain transmission voltages within limits that are generally accepted in the region and consistently adhered to by the Transmission Provider.

Reactive Supply and Voltage Control from Generation or Other Sources Service is to be provided directly by the Transmission Provider (if the Transmission Provider is the Control Area operator) or indirectly by the Transmission Provider making arrangements with the Control Area operator that performs this service for the Transmission Provider's Transmission System. The Transmission Customer must purchase this service from the Transmission Provider or the Control Area operator. A Transmission Customer may satisfy all or part of its obligation through self provision or purchases provided that the self-provided or purchased reactive power reduces the Transmission Provider's reactive power requirements and is from generating facilities under the control of the Transmission Provider or Control Area operator. The Transmission Customer's Service Agreement shall specify any such reactive supply arrangements. To the extent the Control Area operator performs this service for the Transmission Provider, charges to the Transmission Customer are to reflect only a pass-through of the costs charged to the Transmission Provider by the Control Area operator. The Transmission Provider's rates for Reactive Supply and Voltage Control from Generation Sources Services shall be set out in Appendix A to this Schedule.

Given the importance of the procurement or self providing of reactive power, even in a market setting a form of Schedule 2 is found in the tariffs of MISO and PJM, for example. Also, other contractual mechanism, such as Interchange agreements, also are used to ensure transmission customers (such as PSEs and LSEs) provide reactive power, While NERC complied with the Commission's directive to add LSEs to VAR-001-2 R5, a review of this requirement in light of Schedule 2 indicates that the reliability objective of ensuring that PSEs as well as LSEs either acquire or self provide reactive power

resources associated with its transmission service requests is accomplished via Schedule 2, and, therefore, there is no need to reiterate it in VAR-001-2 R5. The repetitive nature of VAR-001-2 R5 is also apparent in the context of how a PSE or LSE generally demonstrates compliance – via screenshots from Open Access Same-Time Information System ("OASIS") reservations that show the mandatory acquiring or self providing of reactive power resources per Schedule 2.

The reliability objective of VAR-001-2 is also accomplished in VAR-001-2 R2 (that is not proposed for retirement) which reads:

> Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, [sic] and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

The Transmission Operator's adherence to R2 is a double check for the obligations under Schedule 2 to ensure there are sufficient reactive power resources to protect the voltage levels under normal and Contingency conditions. This double check, however, does not relieve PESs and LESs from their obligations under Schedule 2 of the OATT or Interchange agreements.

In addition, in the Electric Reliability Council of Texas (ERCOT) region, where there is no FERC approved OATT, reactive power is handled via Section 3.15 of the ERCOT Nodal Protocols that describes how ERCOT establishes a Voltage Profile for the grid, and then in detail explains the responsibilities of the Generators, Distribution Providers and Texas Transmission Service Providers (not to be confused with a NERC TSP), to meet the Voltage Profile and ensure that those entities have sufficient reactive support to do so. There is further Operating Guide detail on the responsibilities for entities to deploy reactive resources approximately, within performance criteria in the Operating Guide Section 3. Thus, as in non-ERCOT regions, ERCOT has protocols that are duplicative of VAR-001-2 R5.

Given the redundant nature of VAR-001-2 R5 it would also assist the ERO compliance program to retire it, so that time and resources can be reallocated to focus on adherence to other Reliability Standard requirements.

Criterion A
VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* OATT.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. VAR-001-2 R5 has not been part of a FFT filing.

2. VAR-001-2 R5 is subject to Standards Development Project 2008-01 Voltage and Reactive Planning Control. Given that Project 2008-01 is not currently active and is only estimated to be completed until the second quarter of 2014 and the purpose of this project does not necessarily include a review of R5, it is appropriate to include VAR-001-2 R5 in the P81 Project. Also, retiring this requirement via P81 Project may facilitate the efficiency of Project 2008-01.

3. This requirement has a High VRF. However, the reliability objective of VAR-001-2 R5 will be accomplished via Schedule 2 of the OATT, ERCOT protocols and R2 of VAR-001-2. Thus, the High VRF is not dispositive, and VAR-001-2 R5 remains appropriate for retirement.

4. VAR-001-2 R5 is in the third tier of the AML.

5. Because VAR-001-2 R5 is redundant with the *pro forma* OATT and ERCOT protocols, (as well as the reliability objective of VAR-001-2 R5 is accomplished via Schedule 2 of the OATT, ERCOT protocols and R2 of VAR-001-2), the retirement of VAR-001-2 R5 does not pose any negative impact to the following NERC published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of VAR-001-2 R5 is neutral regarding whether it promotes a results-based approach because the requirement is results-based, but already covered in the *pro forma* OATT, Schedule 2 and ERCOT protocols.

Accordingly, for the above reasons, it is appropriate to retire VAR-001-2 R5.

V. The Initial Phase Reliability Standards Provided for Informational Purposes

The following requirements are already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the NERC Board of Trustees in November), and, thus, are presented here for informational purposes only. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the NERC Board of Trustees for approval or filed with the Commission or Canadian governmental authorities as part of the P81 Project.

CIP-001-2a R4 Sabotage Reporting

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

Background

CIP-001-1 was filed for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[70] CIP-001-1a was filed for Commission approval on April 21, 2010 in Docket No. RD10-11-000, and was approved by an unpublished letter order on February 2, 2011.[71]

CIP-001-2a was filed for Commission approval as a Regional Variance for the ERCOT Region, containing an interpretation of CIP-001-1, on June 21, 2011 in Docket No. RD11-6-000 and was approved by unpublished letter order on August 2, 2011.[72]

As part of EOP-004-2, on November 5, 2012, stakeholders approved the retirement of CIP-001-2a R4. EOP-004-2 was approved by the NERC Board of Trustees on November 7, 2012. Thus, CIP-001-2a R4 is presented here for informational purposes only.

[70] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[71] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-001-1 —Cyber Security— Sabotage Reporting, Requirement R2, Docket No. RD10-11-000 (February 2, 2011).
[72] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of the Reliability Standard CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity, Docket No. RD11-6-000 (August 2, 2011).

COM-001-1.1 R6- Telecommunications

Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."

Background
COM-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[73] COM-001-1.1 was submitted for Commission approval on February 6, 2009 in Docket No. RD09-2-000 as errata and was approved by unpublished letter order on May 13, 2009.[74]

As part of COM-001-2, on September 17, 2012, stakeholders approved the retirement of COM-001-1.1 R6 in Project 2006-06 (Reliability Coordination). This project is due to be presented to the NERC Board of Trustees in November. Thus, COM-001-1 R6 is presented here for informational purposes only.

EOP-004-1 R1 – Disturbance Reporting

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

Background
EOP-004-1 was submitted to the Commission for approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[75]

As part of EOP-004-2, on November 5, 2012, stakeholders approved the retirement of EOP-001-1 R1. EOP-004-2 was approved by the NERC Board of Trustees on November 7, 2012. Thus, EOP-001-1 R1 is presented here for informational purposes only.

EOP-009-0 R2 – Documentation of Blackstart Generating Unit Test Results

R2. The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

Background

[73] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[74] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Reliability Coordination and Transmission Operations Reliability Standards, Docket No. RD09-2-000 (May 13, 2009).
[75] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

EOP-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[76] In Order No. 749, the Commission approved the retirement of EOP-009-0 as of July 1, 2013, based on the approval of EOP-005-2, which did not carry forward R2 of EOP-009-0. Thus, EOP-009-0 R2 is presented here for informational purposes only.

FAC-008-1 R1.3.5 – Facility Ratings Methodology

R1.3.5. Other assumptions.

Background
FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[77]

"On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No. 693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[78]

FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[79]

FAC-008-3 (which combined FAC-008 and FAC-009) has been approved by the Commission without the "other assumptions" language.[80] Since FAC-008-3 will become effective on January 1, 2013, FAC-008-1 R1.3.5 is presented here for informational purposes only.

PRC-008-0 R1; PRC-008-0 R2 – Underfrequency Load Shedding Equipment Maintenance Programs

R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS

[76] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[77] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[78] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[79] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).
[80] *Id.*

equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.

R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).

Background
PRC-008-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[81]

Under Standards Development Project 2007-17 Protection System Maintenance, which recently passed on August 27, 2012, PRC-008-0 is scheduled to be retired, subsumed and replaced with PRC-005-2. PRC-005-2 will likely be presented to the NERC Board of Trustees in November for approval, and, thus, PRC-008-0 is only presented here for informational purposes.

PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2 – UFLS Performance Following an Underfrequency Event

R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UFLS set points and tripping times.

R1.3. A simulation of the event.

[81] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

R1.4. A summary of the findings.

R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.

Background
PRC-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[82] In Order No. 763 at paragraph 103[83] the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Thus, PRC-009-0 is presented here for informational purposes only.

TOP-001-1a R3 – Reliability Responsibilities and Authorities

R3. Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.

Background
TOP-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved by the Commission on March 16, 2007 in Order No. 693.[84] TOP-001-1a was submitted for approval on July 16, 2010 in Docket No. RM10-29-000 and was approved on September 15, 2011 in Order No. 753.[85]

IRO-001-1a R8 reads:

[82] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[83] *Automatic Underfrequency Load Shedding and Load Shedding Plans Re-liability Standards*, 139 FERC ¶ 61,098 (2012).
[84] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[85] *Electric Reliability Organization Interpretation of Transmission Operations Reliability Standard*, 136 FERC ¶ 61,176, (September 15, 2011) (Order No. 753).

> Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.

Although there is redundancy between TOP-001-1a R3 and IRO-001-1a R8 as related to Reliability Coordinators, this redundancy was addressed in Standards Development Project 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces TOP-001-1a R3 and reads:

> Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued and identified as such by its Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.

TOP-001-2 has been approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-001-1a R3 is presented for informational purposes only.

TOP-005-2a R1 – Operational Reliability Information

R1. As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."

Background

Without directly addressing R1 of TOP-005-1 or TOP-005-2a the Commission approved both versions of TOP-005. [86] A review of the Standards Development Project 2007-03 Real-time Transmission Operations indicates it proposes R1 of TOP-005-1 to be retired. The reasoning provided by the SDT was the following:

[86] Order No. 693 at paragraphs 1648 through 1652 (approval of TOP-005-1); *Mandatory Reliability Standards for Interconnection Reliability Operating Limits*, 134 F.E.R.C. ¶ 61,213 (2011) (approval of TOP-005-2a).

> Confidentiality is not a reliability issue, but a market or business issue. Since this is not a reliability issue, it does not belong in the Reliability Standards and can be deleted.[87]

As stated above, in the context of Project 2007-03, TOP-001-1a was approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-005-2a R1 is presented for informational purposes only.

[87] Mapping Document Project 2007-03 Real-time Operations at page 31 (April 27 2012).

Appendix A

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
BAL-005-0.2b	**R2**	√							√			H		No	No	Yes
CIP-003-3, -4	**R1.2**	√	√							√	√	L	2	No	No	Yes
CIP-003-3, -4	**R3, R3.1 R3.2 R3.3**	√	√		√					√	√	L	3	No	No	Yes
CIP-003-3, -4	**R4.2**	√	√		√				√	√	√	L	3	No	No	Yes
CIP-005-3a, -4a	**R2.6**	√	√		√					√	√	L	1	No	No	Yes
CIP-007-3, -4	**R7.3**	√	√	√							√	L	1	No	No	Yes
EOP-005-2	**R3.1**	√	√				√		√			N/A	2	No	No	Yes
FAC-002-1	**R2**	√	√	√								L	3	No	No	Yes
FAC-008-1	**R2, R3**	√	√			√		√				L	3	No	No	Yes
FAC-008-3	**R4**	√	√			√		√				L	3	No	No	Yes

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
	R5															
FAC-010-2.1	**R5****	√	√			√		√				L		No	No	Yes
FAC-011-2	**R5****	√	√			√		√				L		No	No	Yes
FAC-013-2	**R3**	√	√			√		√				L		No	No	Yes
INT-007-1	**R1.2**	√	√									L		No	No	Yes
IRO-016-1	**R2**	√	√	√								L		No	No	Yes
NUC-001-2	**R9.1** **R9.1.1** **R9.1.2** **R9.1.3** **R9.1.4**	√	√									N/A	3	No	No	Yes
PRC-010-0	**R2**	√	√	√								L		No	No	Yes
PRC-022-1	**R2**	√	√	√								L		No	No	Yes
VAR-001-2	**R5****	√							√			H	3	No	No	Yes

Exhibit F

Summary of the Standard Development Proceedings and Record of Development of Proposed Reliability Standard

Exhibit F — Summary of the Standard Development Proceedings and Record of Development of Proposed Reliability Standard

I. SUMMARY OF THE STANDARD DEVELOPMENT PROCEEDINGS

a. NERC Reliability Standards Development Procedure

The proposed retirement of Reliability Standards was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[74] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[75] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders, and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard, including the retirement of any Requirement in a Reliability Standard, before the Reliability Standard is submitted to the Commission for approval.

b. Overview of the Project 2013-02 Team

When evaluating proposed Reliability Standards and associated modifications, the Commission is expected to give "due weight" to the technical expertise of the ERO.[76] The

---

[74] Order No. 672 at P 334 ("Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's Reliability Standard development process if it is conducted in good faith in accordance with the procedures approved by FERC.").

[75] The NERC Rules of Procedure are available here: http://www.nerc.com/page.php?cid=1%7C8%7C169. The current NERC Standard Processes Manual is available here: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf.

[76] Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824o(d)(2) (2012).

technical expertise of the ERO is derived from the drafting team. For this project, the Team consisted of fifteen industry experts with a diversity of experience. A detailed set of biographical information for each of the team members is included along with the P 81 Team roster in **Exhibit G**. The development record for the P 81 Project is summarized below.

c. First Posting, Informal Comment Period

The draft SAR, which included criteria for retiring or modifying requirements, defined phases for the project, and a suggested list of requirements put together by NERC, the regions, and the trades and their member companies for consideration in Phase I, was posted for an informal comment period from August 3, 2012 through September 4, 2012.

In September, the P81 drafting team met to respond to the comments received and finalize the SAR. The revisions resulted in a list of 38 requirements in 22 Reliability Standard versions being proposed for retirement and an additional 13 requirements included for informational purposes only. The P81 Team also developed a Technical White Paper which includes the justification for retiring the proposed requirements included herein as **Exhibit E**.

d. Second Posting, Formal Comment and Initial Ballot

The project with redlined versions of 22 standards showing 38 requirements proposed to be retired for Phase 2 was posted for a 45-day public comment period and initial ballot from October 25, 2012 through December 10, 2012. The initial ballot for the project received a quorum of 75.77% and a 96.45% approval.

The P 81 Team received 32 sets of comments from 113 people from 64 companies representing 8 of the 10 industry segments. No entity showed that a gap in reliability would result from the retirement of the proposed Reliability Standard requirements. The comments were very supportive of the retirement of the proposed Reliability Standard requirements. A few

entities provided clarifying comments for consideration in the technical white paper, and those comments have been incorporated to enhance the readability and clarity of the technical white paper. Based on the comments, CIP-001-2a R4 and EOP-004-1 R1 will be moved to Section V of the technical paper entitled **"**The Initial Phase Reliability Standards Provided for Informational Purposes," as EOP-004-2 has been filed with regulatory authorities and the EOP-004-2 implementation plan calls for the retirement of CIP-001-2a R4 and EOP-004-1 R1. This resulted in a final list of 34 requirements in 19 Reliability Standard versions.

e. Third Posting, Recirculation Ballot

The project with redlined versions of 20 standards showing 36 requirements proposed to be retired for Phase 3 was posted for a 10-day recirculation ballot from January 8, 2013 through January 17, 2013. The project received a quorum of 84.60% and a 95.22% approval.

f. Board of Trustees Approval

The final project was approved by the NERC Board of Trustees on February 7, 2013.

Project 2013-02
Paragraph 81

Related Files

Status:
Adopted by the NERC Board of Trustees on February 7, 2013 and pending regulatory approval.

Purpose / Industry Need:
This project is in response to paragraph 81 of FERC's March 15, 2012 Order issued on NERC's Find, Fix and Track process. The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES", are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs. Phase 1 of the project identifies Reliability Standard requirements that clearly meet the criteria set forth in the SAR and do not require extensive technical research. Subsequent phases will address Reliability Standard requirements that need additional technical research before retirement or modification.

Draft	Action	Dates	Results	Consideration of Comments
Redline of Standards with Proposed Retirements **(22)** Implementation Plan Clean **(23)** | Redline to Last Posted **(24)** **Supporting Materials:** Technical White Paper Clean **(25)**| Redline to Last Posted **(26)** Redline of VSL Matrix **(27)** Spreadsheet with Proposed Retirements **(28)**	Recirculation Ballot Info **(30)** Vote>>	01/08/13 - 01/17/13 (closed)	Summary **(31)** Ballot Results **(32)**	

Clean Set of Standards with Proposed Retirements **(29)**				
Redline of Standards with Proposed Retirements **(8)** Implementation Plan **(9)** **Supporting Materials:** Final SAR Clean **(10)** | Redline to draft SAR **(11)** Technical White Paper **(12)** Redline of VSL Matrix **(13)** Spreadsheet with Proposed Retirements **(14)** Comment Form (Word) **(15)**	Updated Info **(16)** Initial Ballot >>	11/30/12 - 12/10/12 (closed)	Summary **(18)** Full Record **(19)**	
	Join Ballot Pool>>	10/25/12 - 11/23/12		
	Comment Period Info **(17)** Submit Comments>>	10/25/12 - 12/10/12 (closed)	Comments Received **(20)**	Consideration of Comments **(21)**
Proposed SAR Draft SAR Version 1 **(1)** **Supporting Materials:** Complete Set of Standards with Proposed Retirements	Comment Period Info **(5)** Submit Comments>>	08/03/12 - 09/04/12 (closed)	Comments Received **(6)**	Consideration of Comments **(7)**

for Phase 1 **(2)** Spreadsheet with Proposed Retirements **(3)** Comment Form (Word) **(4)**				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Retirement of Reliability Standard Requirements		
Date Submitted:	June 29, 2012		
SAR Requester Information			
Name:	Brian J. Murphy on behalf of the following:		
Organization:	Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group		
Telephone:	305-442-5132		
SAR Type (Check as many as applicable)			
☐ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated: "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser

SAR Information

risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, the problem this SAR is resolving is to identify Reliability Standards requirements that either: (a) provide little protection to the BPS;[1] (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file the identified Reliability Standard requirements with FERC to have them removed from the FERC-approved list of Reliability Standards.

In addition to addressing P81, this SAR is also consistent with Recommendation #4 set forth in *NERC's Recommendations to Improve The Standards Development Process* at page 12 (April 2012), which states:

> **Recommendation 4: Standards Product Issues** — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

[1] Given NERC's Reliability Standards are based on the definition of a Bulk Electric System (BES), the remainder of this SAR will use the term BES rather than Bulk Power System or BPS.

SAR Information
Purpose or Goal (How does this request propose to address the problem described above?):
The SAR addresses the problem identified above by: (1) Setting forth specific criteria (below) to evaluate whether a Reliability Standard requirement provides little protection to BES reliability or is unnecessary or redundant. (2) Establishing a multi-phased process for addressing these Reliability Standard requirements. During the Initial Phase, the Standards Drafting Team will identify those Reliability Standard requirements that easily satisfy the criteria and either recommend: (a) the retirement of the requirement[2] or (b) a modification to the requirement,[3] while future phases will identify the remaining Reliability Standard requirements that satisfy the criteria, but could not be included in the Initial Phase due to the need for additional analysis or a modification of language. This multi-phased approach is also proposed to address FERC's interest in increasing the efficiency of the ERO compliance program, so that the first set of identified Reliability Standard requirements may be filed with FERC on an expedited basis, and, therefore, start increasing ERO efficiencies as soon as practical. (3) To facilitate the Initial Phase of the Standard Drafting Team's process, a list of Reliability Standard requirements that appear to easily satisfy the criteria are set forth below. (4) During each phase, as a list of Reliability Standard requirements is identified and passes through the Standards Development Process, the Standards Drafting Team[4] will also assist NERC staff to file these requirements with FERC so the requirements are removed from the FERC-approved list, including providing additional technical justification, as needed.

[2] The Standards Drafting Team will work with NERC staff to determine the manner to eliminate the identified Reliability Standards requirements.

[3] Given the expedited nature of the Initial Phase, it is unlikely there will be a large number of modifications considered, and the Standards Drafting Team may decide to defer all requested modifications to subsequent phases.

[4] While this SAR applies to all phases of the P81 project, it is understood that the composition of the Standard Drafting Team may need to change or be supplemented in subsequent phases depending on the technical expertise required.

SAR Information
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
The objectives of this SAR for all phases of this project are to retire or modify FERC-approved Reliability Standard requirements that provide little protection to the reliable operations of the BES, are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The scope of this SAR is all FERC-approved Reliability Standards.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The Standard Drafting Team shall implement a phased process. The Initial Phase shall identify all FERC-approved Reliability Standard requirements that easily satisfy the criteria set forth below, while future phases shall identify FERC-approved Reliability Standard requirements that satisfy the criteria set forth below, but could not be included in the Initial Phase due to the need for additional analysis or an editing of language. During each phase the Standards Drafting Team shall identify Reliability Standard requirements that satisfy **both**: (A) the overarching criteria and (B) at least one of the technical criteria. In addition, for all phases, the Standards Drafting Team shall also consider the data and reference points set forth below in Criterion C when deciding whether a Reliability Standard requirement should be retired or modified. **A. Overarching Criterion:** In the event no responsible entity performed the FERC-approved Reliability Standard requirement, there would be little or no impact to the protection or reliable operation of the BES. Section 215(a)(4) of the Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

SAR Information

B. Technical Criteria:

1. Administrative

The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

2. Data Collection/Data Retention

The Reliability Standard requirement requires responsible entities to collect or retain data and does not contribute to: (a) the reliable operation of the BES or (b) an effective compliance enforcement processes. These are requirements that obligate responsible entities to retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes or addressed in the data retention sections of Reliability Standards.

3. Purely Documentation

The Reliability Standard requirement requires responsible entities to develop a document (*e.g.,* plan, policy or procedure) which is not necessary to protect BES reliability.

4. Purely Reporting

The Reliability Standard requirement obligates responsible entities to report out to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernable impact on promoting reliable operation of the BES and if the entity failed to meet this requirement it would have little impact on the reliable operation of the BES.

5. Periodic Updates

The Reliability Standard requirement requires responsible entities to periodically update (*e.g.,* annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

6. Commercial or Business Practice

The Reliability Standard requirement is a commercial or business practice, *e.g.,* better served as a

SAR Information
NAESB standard or as part of NAESB Electric Industry Registry (EIR). **7. Redundant** The Reliability Standard requirement is redundant with either another Reliability Standard requirement or governmental regulation (*e.g.,* Open Access Transmission Tariff, NAESB, etc.). **8. Hinders the protection or reliable operation of the BES** The Reliability Standard requirement requires responsible entities to conduct an activity or task that hinders, distracts or is counterproductive to the protection or reliable operation of the BES. **9. Little, if any, value as a reliability requirement** The tasks or activities in the Reliability Standard requirement do little, if anything, to promote the protection the BES. **C. Additional data and reference points** In those instances when there is the need for additional information to assist in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B, the Standards Drafting Team shall consider the following data and reference points to make a more informed decision: 1. Was the Reliability Standard requirement part of a Find, Fix and Track filing? 2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project? 3. What is the Violation Risk Factor of the Reliability Standard requirement? 4. In which tier of the Actively Monitored Standards does the Reliability Standard requirement fall? 5. Any negative impact on NERC's published and posted reliability principles?

SAR Information

6. Any negative impact on the defense in depth protection of the BES?

7. Does the retirement or modification promote results or performance-based Reliability Standards?

To facilitate the Standard Drafting Team's consideration of the above questions, NERC staff will provide the team with relevant known data and statistics.

To facilitate the Standard Drafting Team's Initial Phase, below is a list of Reliability Standard requirements that appear to satisfy both Criteria A and B, with consideration of Criterion C. To assist the Team's review of these requirements, Criterion B coding is provided, along with a brief statement explaining why the requirement provides little protection to the BES, is unnecessary or is redundant.

List of Phase One Reliability Standard requirements that satisfy both Criteria A and B, with consideration of Criterion C

To be retired:

BAL-005-0.1b R2

Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

Criterion B 7.

Statement: BAL-005-0.1b is redundant with the Control Performance Standard defined in BAL-001 R1 and R2. This is also redundant in that it is measured by whether or not BAL-001 R1 and R2 are met.

SAR Information
Conclusion: This is redundant with the Control Performance Standard defined in BAL-001 R1 and R2. This is also redundant in that it is measured by whether or not BAL-001 R1 and R2 are met. This may be double jeopardy in that failure to achieve compliance with BAL-001 R1 and R2 could imply failure of this standard as well. This is misleading in requiring entities to maintain Regulating Reserve, but providing no way to measurably comply, apart from achieving compliance with BAL-001 R1 and R2. **CIP-001-2a R4.** Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances. Criterion B 1, 2, 3, 8 and 9. **Statement:** CIP-001-2a is administrative, documentation and data collection in nature, because the establishment of communication contacts, in and of itself, with the FBI and RCMP has little or no impact on protection or the reliable operation of the BES. Instead, compliance with R1-R3 of CIP-001-2a provides the actions that responsible entities take to protect the BES in the event of sabotage. Specifically, R1 through R3 require that the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity to have procedures for the recognition of sabotage, reporting of sabotage and communication of sabotage events to appropriate parties in the Interconnection, which may include local law enforcement, the FBI, etc. Thus, in CIP-001-2a, R1 through R3 serve a reliability function, while R4 is a static, administrative requirement that has no clear results-based nexus to protecting the Bulk Electric System (BES). **Conclusion**: Since this requirement provides little protection to the BES and is administrative in nature, Requirement 4 should be removed from Reliability Standard CIP-001-2a. **CIP-003-3, -4 R1.2** The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

SAR Information

Criterion B 1.

Statement: Whether there is a robust CIP compliance plan on which employees are trained may impact reliability, not whether the cyber security policy is readily available. Employees that are responsible for executing the cyber security policy are required to undergo a variety of training, follow multiple processes and procedures that are already required by the CIP requirements. Simply requiring that the policy be readily available is an administrative task that provides little, if any, benefit to reliability of the BES.

Conclusion: Since this requirement provides little protection to the BES and is purely administrative in nature, Requirement 1.2 should be removed from Reliability Standards CIP-003-3 and CIP-003-4.

CIP-003-3, -4 R3, R3.1, R3.2, R3.3

R3 Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1 Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2 Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3 Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Criterion B 1, 3 and 8.

Statement: Over time, these exception requirements have proven to not be useful and have been

SAR Information
subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements. **Conclusion:** For regulatory efficiency, since these requirements provide little protection to the BES and are open to misinterpretation, in addition to being entirely documentation, Requirement 3 and its subrequirements should be removed from Reliability Standard CIP-003-3 and CIP-003-4. **CIP-003-3, -4 R4.2.** The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. Criterion B 1, 3 and 7. **Statement:** CIP-003-3, -4 already requires the classification of information associated with Critical Cyber Assets, which makes R4.2 redundant. The only difference in R4.2 is the term, "based on the sensitivity" has been added. The addition of this term can be viewed as overly managing the responsible entities' process of classification or simply not adding sufficient value to reliability to require new requirement over and above R4. **Conclusion:** Since these requirements are redundant and provide little protection to the BES, Requirement 4.2 should be removed from both Reliability Standards CIP-003-3 and CIP-003-4. **CIP-005-3a, -4a R2.6.** Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. Criterion B 1, 3, 8 and 9.

SAR Information

Statement: Over time, the banner requirement (or no trespass sign) has not been shown to be useful or consistent with a results-based approach to implementing a cyber security program. Additionally, it is administrative in nature.

Conclusion: Since this requirement provides little protection to the BES and is purely administrative in nature, Requirement R2 should be removed from Reliability Standards CIP-005-3a and CIP-005-4.

CIP-007-3, -4 R7.3

The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Criterion B 2.

Statement: CIP-007-3, -4 R7.3 is evidence collection and possible for inclusion in an RSAW.

Conclusion: Since this requirement provides little protection to the BES and is data collection in nature, it should be removed from CIP-007-3, -4.

COM-001-1.1 R6.

Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."

Criterion B 6.

Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether it employs a specific business practice such as the NERCNet. NOTE: This requirement is proposed for removal per Project 2006-06 (Reliability Coordination) with the rationale: "The RC SDT is recommending that R6 be retired. This is an ERO procedural issue and should not be in a reliability standard. It should be included in the ERO Rules of Procedure."

SAR Information

Conclusion: Since this requirement provides little protection to the BES and is more appropriate as a Commercial and Business Practice, Requirement 6 should be removed from Reliability Standard COM-001-1.1.

EOP-004-1 R1.

Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

Criterion B 1, 3 and 4.

Statement: Whether or not there is a Regional Entity procedure to report disturbances has no impact on reliability. In other words, while a procedure for the collection of reports on disturbances may be useful information for purposes of Regional Entities to stay informed during events, is not an activity that protects the reliability of BES. The collection of such information should be established outside mandatory Reliability Standards.

Conclusion: Since this requirement provides little protection to the BES and is purely documentation, Requirement 1 should be removed from Reliability Standard EOP-004-1.

EOP-005-2 R3.1.

If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

Criterion B 1, 5, 7 and 9.

Statement: EOP-005-2 R3 reads: "Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule." This requirement requires the Transmission Operator to submit its restoration plan to the Reliability

SAR Information
Coordinator whether or not there have been changes. Therefore, R3.1 only adds a duplicative administrative burden for the entity to also confirm that there were no changes based upon another possible pre-determined schedule. Whether or not there was a change from year to year in the restoration plan will be documented in the revision history of the restoration plan, and thus the Reliability Coordinator will be able to ascertain whether or not there were changes based on R3. Thus, EOP-005-2 R3.1 provides little, if any, value to promoting the protection of the BES. **Conclusion:** For regulatory efficiency, and since this requirement appears redundant to R3, Requirement 3.1 should be removed from Reliability Standard EOP-005-2. **EOP-009-0 R2.** The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC. Criterion B 4. **Statement:** The requirement to report blackstart test results to the Regional Entity and NERC has no impact on reliability. If the Regional Entity desires to review or track this information, a better vehicle to obtain it is via a Compliance Audit or Spot-Check, or some other compliance monitoring procedure. **Conclusion:** For regulatory efficiency and since this requirement is purely a reporting activity, Requirement 2 should be removed from Reliability Standard EOP-009-0. **FAC-002-1 R2.** The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

SAR Information

Criterion B 2, 3 and 4.

Statement: Requiring the retention of studies for three years has no impact on protecting or the reliable operation of the BES, and is merely a data retention requirement that is better suited to be considered during an audit or in the context of compliance monitoring.

Conclusion: Since this requirement provides little protection to the BES and is purely data collection/retention, Requirement 2 should be removed from Reliability Standard FAC-002-1.

FAC-008-1 R1.3.5.

Other assumptions.

Criterion B 8.

Statement: The term “other assumptions" in the context of facility ratings is very close to meaningless from a technical standpoint, generic and, therefore, yields no protection of the BES.

Conclusion: Since this requirement provides little or no protection to the BES and is unnecessary, Requirement 1.3.5 should be removed from Reliability Standard FAC-008-1.

FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5

FAC-008-1 R2 The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

FAC-008-1 R3 If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner’s or Generator Owner’s Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a

SAR Information
written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. FAC-008-3 R4 Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. FAC-008-3 R5 If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. Criterion B 1, 2, 4 and 6. **Statement:** For purposes of reliability, facility ratings are transmitted and used via the FAC (System Operating Limits), MOD and TPL Standards,[5] and posting the rating methodology for comment and responding to comments in and of itself has no reliability benefit. Furthermore, these requirements do not appear appropriate given the possible commercial or market related implications of sharing and debating with a competitor the facility ratings methodology of a facility.

[5] MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-02 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element. Also, FAC-008-3 R7 and R8 require the transmission of facility ratings to reliability entities.

SAR Information
Conclusion: For regulatory efficiency and possible commercial or market implications in sharing the facility ratings, and since these requirements are purely administrative in nature along with reporting activities, Requirements R2 and R3 of Reliability Standard FAC-008-1 and Requirements 4 and 5 of Reliability Standard FAC-008-3 should be removed from the Standards. **FAC-013-2 R3** If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. Criterion B 1, 2, 4 and 6. **Statement:** Similar to the concerns with FAC-008, the FAC-013-2 requirement to reply to comments on a transfer capability methodology has no reliability benefit, and, moreover, a back and forward on transfer capability could have commercial or market implications. **Conclusion:** For regulatory efficiency and possible commercial or market implications in sharing transfer capability methodology, and since these requirements are purely administrative in nature along with reporting activities, Requirement R3 of Reliability Standard FAC-013-2 should be removed from the Standards. **INT-007-1 R1.2** All reliability entities involved in the Arranged Interchange are currently in the NERC registry. Criterion B 1 **Statement:** INT-007-1, R1.2 is administrative in nature, and adds little to reliability.

SAR Information
Conclusion: Since INT-007-1 R1.2 provides little protection to the BES, it should be removed. **IRO-016-1 R2** The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both. Criterion B 2. **Statement:** IRO-016-1 R2 is an evidence requirement. Candidate to go into RSAW. **Conclusion:** Since IRO-016-1 R2 provides little protection to the BES and is data collection in nature, it should be removed. **MOD-004-1 R1; MOD-004-1 R1.1; MOD-004-1 R1.2; MOD-004-1 R1.3; MOD-004-1 R2; MOD-004-1 R3; MOD-004-1 R3.1; MOD-004-1 R3.2; MOD-004-1 R4; MOD-004-1 R4.1; MOD-004-1 R4.2; MOD-004-1 R5; MOD-004-1 R5.1; MOD-004-1 R5.2; MOD-004-1 R6; MOD-004-1 R6.1; MOD-004-1 R6.2; MOD-004-1 R7; MOD-004-1 R8; MOD-004-1 R9; MOD-004-1 R9.1; MOD-004-1 R9.2; MOD-004-1 R10; MOD-004-1 R11; MOD-004-1 R12; MOD-004-1 R12.1; MOD-004-1 R12.2; MOD-004-1 R12.3.** R1 The Transmission Service Provider that maintains CBM shall prepare and keep current a "Capacity Benefit Margin Implementation Document" (CBMID) that includes, at a minimum, the following information: [Time Horizon: Operations Planning, Long-term Planning] R1.1 The process through which a Load-Serving Entity within a Balancing Authority Area associated with the Transmission Service Provider, or the Resource Planner associated with that Balancing Authority Area, may ensure that its need for Transmission capacity to be set aside as CBM will be reviewed and accommodated by the Transmission Service Provider to the extent Transmission capacity is available. R1.2 The procedure and assumptions for establishing CBM for each Available Transfer Capability (ATC)

SAR Information
Path or Flowgate. R1.3 The procedure for a Load-Serving Entity or Balancing Authority to use Transmission capacity set aside as CBM, including the manner in which the Transmission Service Provider will manage situations where the requested use of CBM exceeds the amount of CBM available. R2 The Transmission Service Provider that maintains CBM shall make available its current CBMID to the Transmission Operators, Transmission Service Providers, Reliability Coordinators, Transmission Planners, Resource Planners, and Planning Coordinators that are within or adjacent to the Transmission Service Provider's area, and to the Load Serving Entities and Balancing Authorities within the Transmission Service Provider's area, and notify those entities of any changes to the CBMID prior to the effective date of the change. [Time Horizon: Operations Planning] R3 Each Load-Serving Entity determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by: [Time Horizon: Operations Planning] R3.1 Using one or more of the following to determine the GCIR: Loss of Load Expectation (LOLE) studies Loss of Load Probability (LOLP) studies Deterministic risk-analysis studies Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities R3.2 Identifying expected import path(s) or source region(s). R4 Each Resource Planner determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by: [Time Horizon: Operations Planning]

SAR Information
R4.1 Using one or more of the following to determine the GCIR: Loss of Load Expectation (LOLE) studies Loss of Load Probability (LOLP) studies Deterministic risk-analysis studies Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities R4.2 Identifying expected import path(s) or source region(s). R5 At least every 13 months, the Transmission Service Provider that maintains CBM shall establish a CBM value for each ATC Path or Flowgate to be used for ATC or Available Flowgate Capability (AFC) calculations during the 13 full calendar months (months 2-14) following the current month (the month in which the Transmission Service Provider is establishing the CBM values). This value shall: [Time Horizon: Operations Planning] R5.1 Reflect consideration of each of the following if available: Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Service Provider's area Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Service Provider's area Any reserve margin or resource adequacy requirements for loads within the Transmission Service Provider's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities R5.2 Be allocated as follows: For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners

SAR Information
For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Service Provider R6 At least every 13 months, the Transmission Planner shall establish a CBM value for each ATC Path or Flowgate to be used in planning during each of the full calendar years two through ten following the current year (the year in which the Transmission Planner is establishing the CBM values). This value shall: [Time Horizon: Long-term Planning] R6.1 Reflect consideration of each of the following if available: Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Planner's area Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Planner's area Any reserve margin or resource adequacy requirements for loads within the Transmission Planner's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities R6.2 Be allocated as follows: For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Planner. R7 Less than 31 calendar days after the establishment of CBM, the Transmission Service Provider that maintains CBM shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the Transmission Service Provider's system of the amount of CBM set aside. [Time Horizon: Operations Planning]

SAR Information
R8 Less than 31 calendar days after the establishment of CBM, the Transmission Planner shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the system being planned by the Transmission Planner of the amount of CBM set aside. [Time Horizon: Operations Planning] R9 The Transmission Service Provider that maintains CBM and the Transmission Planner shall each provide (subject to confidentiality and security requirements) copies of the applicable supporting data, including any models, used for determining CBM or allocating CBM over each ATC Path or Flowgate to the following: [Time Horizon: Operations Planning, Long-term Planning] R9.1 Each of its associated Transmission Operators within 30 calendar days of their making a request for the data. R9.2 To any Transmission Service Provider, Reliability Coordinator, Transmission Planner, Resource Planner, or Planning Coordinator within 30 calendar days of their making a request for the data. R10 The Load-Serving Entity or Balancing Authority shall request to import energy over firm Transfer Capability set aside as CBM only when experiencing a declared NERC Energy Emergency Alert (EEA) 2 or higher. [Time Horizon: Same-day Operations] R11 When reviewing an Arranged Interchange using CBM, all Balancing Authorities and Transmission Service Providers shall waive, within the bounds of reliable operation, any Real-time timing and ramping requirements. [Time Horizon: Same-day Operations] R12 The Transmission Service Provider that maintains CBM shall approve, within the bounds of reliable operation, any Arranged Interchange using CBM that is submitted by an “energy deficient entity ” under an EEA 2 if: [Time Horizon: Same-day Operations] R12.1 The CBM is available

SAR Information
R12.2 The EEA 2 is declared within the Balancing Authority Area of the "energy deficient entity," and R12.3 The Load of the "energy deficient entity" is located within the Transmission Service Provider's area. Criterion B 6. **Statement:** Capacity Benefit Margin (CBM) is better integrated in marketing functions and is not a reliability function. In the NERC TOP-002 Operations Planning Standard, Requirement R1 specifies that the Transmission Operator shall have an Operating Planning Analysis that represents projected System conditions to assess planned operation for the next day that do not exceed Facility Ratings or Stability Limits for anticipated normal and contingency events. Further, the CBM standard is redundant to the TOP-002 R1 where the marketer would schedule their transmission reserve within the limits established by the Transmission Operator. The Transmission Operator ensures that the established reserve along with other identified schedules are modeled to anticipate next-day conditions and remain within established operating limits. In addition, this Standard is not necessary for the support of BES reliability as evidenced by the fact that of the entities that once used CBM, many dropped it when it became effective due to the unnecessary burdens it placed on the entities. **Conclusion:** The requirements above relate to commercial and market issues regulated under OATT. Furthermore, they provide little protection to the BES and unnecessary as part of NERC Reliability Standards. Requirements 1 through 12 and associated subrequirements should be removed from Reliability Standard MOD-004-1. **NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4** R9.1 Administrative elements:

SAR Information
R9.1.1 Definitions of key terms used in the agreement. R9.1.2 Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. R9.1.3 A requirement to review the agreement(s) at least every three years. R9.1.4 A dispute resolution mechanism. Criterion B 1, 3, 5, 6. **Statement:** These requirements of NUC-001-2 do not address reliability, rather they address administrative and commercial terms of an agreement. Given there is no clear nexus between these requirements and reliability, they should be retired. **Conclusion:** Since these requirements are purely administrative in nature, provide for a periodic update and commercial terms of the agreement, they provide little protection to the BES. Requirement 9.1 and associated subrequirements should be removed from Reliability Standard NUC-001-2. **PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2.** PRC-008-0 R1 The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance. PRC-008-0 R2 The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability

SAR Information
Organization and NERC on request (within 30 calendar days). PRC-009-0 R1 The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to: PRC-009-0 R1.1 A description of the event including initiating conditions. PRC-009-0 R1.2 A review of the UFLS set points and tripping times. PRC-009-0 R1.3 A simulation of the event. PRC-009-0 R1.4 A summary of the findings. PRC-009-0 R2 The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event. PRC-010-0 R2 The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). PRC-022-1 R2 Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

SAR Information
Criterion B 4, 9. **Statement:** Since UVLS and UFLS information is being collected under event analysis, and also PRC-009-0 will become inactive September 30, 2013 and replaced by PRC-006-1, the above requirements add little to reliability. **Conclusion:** Since PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 provides little protection to the BES and better handled under event analysis and lessons learned papers, it should be removed. **TOP-001-1a R3** Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions. Criterion B 7. **Statement:** TOP-001-1a R3 is redundant with IRO-001-1a R8. NOTE: per project 2007-03 (Real-time Operations), this requirement was removed from TOP-001-1a and proposed to be replaced by IRO-001-3, R2, R3, R4. **IRO-001-1a R8 reads:** Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or

SAR Information
Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions. The next proposed version of IRO-001 for this requirement also reads the same. As is apparent from a comparison of the two requirements, there is no need for TOP-001-1a R3 which is duplicative of IRO-001-1a R8. Also, in the next proposed version of TOP-001, Reliability Coordinator has been deleted from this requirement. **Conclusion:** Requirement 3 is redundant to Reliability Standard IRO-001-1a R8 and should be removed from Reliability Standard TOP-001-1a. **TOP-005-2a R1** As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data." Criterion B 3. **Statement:** TOP-005-2a R1 is better suited for ROP than reliability requirement. **Conclusion**: Since TOP-005-2a R1 provides little protection to the BES and is purely documentation in nature, it should be removed. **VAR-002-WECC-1 R2; VAR-501-WECC-1 R2** VAR-002-WECC-1 R2 Generator Operators and Transmission Operators shall have documentation identifying the number of hours excluded for each requirement R1.1 through R1.10. VAR-501-WECC-1 R2 Generator Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.12.

SAR Information
Criterion B 3 and 4. **Statement:** Communication of the status of AVR and PSS with the Transmission Operator may impact reliability, but not documenting or reporting out of this information to a Regional Entity. If the Regional Entity desires to review or track the AVR and PSS hours, such information should be collected via vehicles other than the Reliability Standards, such as Compliance Audits, Spot-Checks and other compliance monitoring procedures. **Conclusion:** For regulatory efficiency and since the requirements are purely documentation and reporting activities, Requirement 2 in Regional Reliability Standards VAR-002-WECC-1 and VAR-501-WECC-1 should be removed from the Standards.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☒ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of responsible entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability

Reliability Functions		
		evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☒	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☒	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☒	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☒	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

Reliability and Market Interface Principles	
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☒	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	

A. Introduction

1. **Title:** **Automatic Generation Control**

2. **Number:** BAL-005-0.1b

3. **Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.

4. **Applicability:**

   4.1. Balancing Authorities

   4.2. Generator Operators

   4.3. Transmission Operators

   4.4. Load Serving Entities

5. **Effective Date:** May 13, 2009

B. Requirements

R1. All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.

R1.1. Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.

R1.2. Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.

R1.3. Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

R3. A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.

R4. A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.

R5. A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.

R6. The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

R7. The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.

R8. The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.

R8.1. Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.

R9. The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.

R9.1. Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.

R10. The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.

R11. Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.

R12. Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.

R12.1. Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.

R12.2. Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.

R12.3. Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.

R13. Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.

R14. The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.

R15. The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

R16. The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

1.1.1. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.

1.1.2. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

1.3.1. Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.

1.3.2. Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition

Appendix 1

Request: *PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:*

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

BAL-005-1

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25% of full scale
Remote terminal unit	≤ 0.25% of full scale
Potential transformer	≤ 0.30% of full scale
Current transformer	≤ 0.50% of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to "annually check and calibrate" does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to "annually check and calibrate" the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation:

As noted in the existing interpretation, BAL-005-1 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system operator. Frequency inputs from other sources that are for reference only are excluded. The time error and frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

A. Introduction

1. **Title:** **Sabotage Reporting**

2. **Number:** CIP-001-2a

3. **Purpose:** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

   4.6. Transmission Owners (only in ERCOT Region).

   4.7. Generator Owners (only in ERCOT Region).

5. **Effective Date:** ERCOT Regional Variance will be effective the first day of the first calendar quarter after applicable regulatory approval.

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance:

2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. Level 2: Not applicable.

2.3. Level 3: Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. Level 4:.Not applicable.

E. ERCOT Interconnection-wide Regional Variance

Requirements

EA.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

EA.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

EA.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

EA.4. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall establish communications contacts with local Federal Bureau of Investigation (FBI) officials and develop reporting procedures as appropriate to their circumstances.

Measures

M.A.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement EA1.

M.A.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements EA2 and EA3.

M.A.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to, procedures, policies, a letter of understanding, communication records,

or other equivalent evidence that will be used to confirm that it has established communications contacts with the local FBI officials to communicate sabotage events (Requirement EA4).

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity shall be responsible for compliance monitoring.

1.2. Data Retention

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended
1	April 4, 2007	Regulatory Approval — Effective Date	New
1a	February 16, 2010	Added Appendix 1 — Interpretation of R2 approved by the NERC Board of Trustees	Addition
1a	February 2, 2011	Interpretation of R2 approved by FERC on February 2, 2011	Same addition
	June 10, 2010	TRE regional ballot approved variance	By Texas RE
	August 24, 2010	Regional Variance Approved by Texas RE Board of Directors	
2a	February 16, 2011	Approved by NERC Board of Trustees	

2a	August 2, 2011	FERC Order issued approving Texas RE Regional Variance	

Appendix 1

Requirement Number and Text of Requirement
CIP-001-1: **R2**. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.
Question
Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?
Response
The drafting team interprets the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. For example, reporting responsibilities result from NERC standards IRO-001 Reliability Coordination — Responsibilities and Authorities, COM-002-2 Communication and Coordination, and TOP-001 Reliability Responsibilities and Authorities, among others. Obligations to report could also result from agreements, processes, or procedures with other parties, such as may be found in operating agreements and interconnection agreements. The drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 Requirement R2. Regarding "who within the Interconnection hierarchy deems parties to be appropriate," the drafting team knows of no interconnection authority that has such a role.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-3

3. Purpose: Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-003-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-3 Requirement R2.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager’s delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented	A senior manager’s delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within thirty calendar days of the effective date.	
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3.	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1.	LOWER	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
R3.2.	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3.	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	The Responsible Entity has established but not documented a change	The Responsible Entity has established but not documented both a change control process and configuration management	The Responsible Entity has not established and documented a change control process OR	The Responsible Entity has not established and documented a change control process AND

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		control process OR The Responsible Entity has established but not documented a configuration management process.	process.	The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a configuration management process.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-3a

3. Purpose: Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability

4.1. Within the text of Standard CIP-005-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-3, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-3 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity	

		shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation
3a	02/02/11	Approved by FERC	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal

Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	and Standard CIP-009-4.	and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter.		
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6.	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.			
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to designated response personnel.	Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	Revised.
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"
4a	4/19/12	FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

3. Purpose: Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-007-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-3 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical)	

		Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, **but did not document** that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).

		testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).		
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.
R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program **but** did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.

R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.

R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
R5.1.1.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

			manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).		
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 **but** did not maintain records as specified in R7.3.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A
R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3.	LOWER	N/A	N/A	N/A	N/A

R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A
R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	

A. Introduction

1. **Title:** **Telecommunications**

2. **Number:** COM-001-1.1

3. **Purpose:** Each Reliability Coordinator, Transmission Operator and Balancing Authority needs adequate and reliable telecommunications facilities internally and with others for the exchange of Interconnection and operating information necessary to maintain reliability.

4. **Applicability**

   4.1. Transmission Operators.

   4.2. Balancing Authorities.

   4.3. Reliability Coordinators.

   4.4. NERCNet User Organizations.

5. **Effective Date:** May 13, 2009

B. Requirements

R1. Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:

R1.1. Internally.

R1.2. Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.

R1.3. With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.

R1.4. Where applicable, these facilities shall be redundant and diversely routed.

R2. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.

R3. Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.

R4. Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing Authorities may use an alternate language for internal operations.

R5. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.

R6. Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001, “NERCNet Security Policy.”

C. Measures

M1. Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include, but is not limited to communication facility test-procedure documents, records of testing, and maintenance records for communication facilities or equivalent that will be used to confirm that it manages, alarms, tests and/or actively monitors vital telecommunications facilities. (Requirement 2 part 1)

M2. The Reliability Coordinator, Transmission Operator or Balancing Authority shall have and provide upon request evidence that could include, but is not limited to operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent, that will be used to determine compliance to Requirement 4.

M3. Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have and provide upon request its current operating instructions and procedures, either electronic or hard copy that will be used to confirm that it meets Requirement 5.

M4. The NERCnet User Organization shall have and provide upon request evidence that could include, but is not limited to documented procedures, operator logs, voice recordings or transcripts of voice recordings, electronic communications, etc that will be used to determine if it adhered to the (User Accountability and Compliance) requirements in Attachment 1-COM-001. (Requirement 6)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations

Regional Reliability Organizations shall be responsible for compliance monitoring of all other entities

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 calendar days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

For Measure 1 each Reliability Coordinator, Transmission Operator, Balancing Authority shall keep evidence of compliance for the previous two calendar years plus the current year.

For Measure 2 each Reliability Coordinator, Transmission Operator, and Balancing Authority shall keep 90 days of historical data (evidence).

For Measure 3, each Reliability Coordinator, Transmission Operator, Balancing Authority shall have its current operating instructions and procedures to confirm that it meets Requirement 5.

For Measure 4, each Reliability Coordinator, Transmission Operator, Balancing Authority and NERCnet User Organization shall keep 90 days of historical data (evidence).

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor.

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

Attachment 1 — COM-001 — NERCnet Security Policy

2. Levels of Non-Compliance for Transmission Operator, Balancing Authority or Reliability Coordinator

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: There shall be a separate Level 3 non-compliance, for every one of the following requirements that is in violation:

2.3.1 The Transmission Operator, Balancing Authority or Reliability Coordinator used a language other then English without agreement as specified in R4.

2.3.2 There are no written operating instructions and procedures to enable continued operation of the system during the loss of telecommunication facilities as specified in R5.

2.4. Level 4: Telecommunication systems are not actively monitored, tested, managed or alarmed as specified in R2.

3. Levels of Non-Compliance — NERCnet User Organization

3.1. Level 1: Not applicable.

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable.

3.4. Level 4: Did not adhere to the requirements in Attachment 1-COM-001, NERCnet Security Policy.

E. Regional Differences

None Identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata

1	November 1, 2006	Adopted by Board of Trustees	Revised
1	April 6, 2007	Requirement 1, added the word “for” between “facilities” and “the exchange.”	Errata
1.1	October 29, 2008	BOT adopted errata changes; updated version number to “1.1”	Errata

Attachment 1 — COM-001 — NERCnet Security Policy

Policy Statement
The purpose of this NERCnet Security Policy is to establish responsibilities and minimum requirements for the protection of information assets, computer systems and facilities of NERC and other users of the NERC frame relay network known as "NERCnet." The goal of this policy is to prevent misuse and loss of assets.

For the purpose of this document, information assets shall be defined as processed or unprocessed data using the NERCnet Telecommunications Facilities including network documentation. This policy shall also apply as appropriate to employees and agents of other corporations or organizations that may be directly or indirectly granted access to information associated with NERCnet.

The objectives of the NERCnet Security Policy are:

- To ensure that NERCnet information assets are adequately protected on a cost-effective basis and to a level that allows NERC to fulfill its mission.
- To establish connectivity guidelines for a minimum level of security for the network.
- To provide a mandate to all Users of NERCnet to properly handle and protect the information that they have access to in order for NERC to be able to properly conduct its business and provide services to its customers.

NERC's Security Mission Statement
NERC recognizes its dependency on data, information, and the computer systems used to facilitate effective operation of its business and fulfillment of its mission. NERC also recognizes the value of the information maintained and provided to its members and others authorized to have access to NERCnet. It is, therefore, essential that this data, information, and computer systems, and the manual and technical infrastructure that supports it, are secure from destruction, corruption, unauthorized access, and accidental or deliberate breach of confidentiality.

Implementation and Responsibilities
This section identifies the various roles and responsibilities related to the protection of NERCnet resources.

NERCnet User Organizations
Users of NERCnet who have received authorization from NERC to access the NERC network are considered users of NERCnet resources. To be granted access, users shall complete a User Application Form and submit this form to the NERC Telecommunications Manager.

Responsibilities
It is the responsibility of NERCnet User Organizations to:

- Use NERCnet facilities for NERC-authorized business purposes only.
- Comply with the NERCnet security policies, standards, and guidelines, as well as any procedures specified by the data owner.
- Prevent unauthorized disclosure of the data.
- Report security exposures, misuse, or non-compliance situations via Reliability Coordinator Information System or the NERC Telecommunications Manager.
- Protect the confidentiality of all user IDs and passwords.
- Maintain the data they own.
- Maintain documentation identifying the users who are granted access to NERCnet data or applications.
- Authorize users within their organizations to access NERCnet data and applications.

- Advise staff on NERCnet Security Policy.
- Ensure that all NERCnet users understand their obligation to protect these assets.
- Conduct self-assessments for compliance.

User Accountability and Compliance
All users of NERCnet shall be familiar and ensure compliance with the policies in this document.

Violations of the NERCnet Security Policy shall include, but not be limited to any act that:

- Exposes NERC or any user of NERCnet to actual or potential monetary loss through the compromise of data security or damage.
- Involves the disclosure of trade secrets, intellectual property, confidential information or the unauthorized use of data.

Involves the use of data for illicit purposes, which may include violation of any law, regulation or reporting requirement of any law enforcement or government body.

A. Introduction

1. **Title:** **Disturbance Reporting**

2. **Number:** EOP-004-1

3. **Purpose:** Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

   4.6. Regional Reliability Organizations.

5. **Effective Date:** January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1	March 22, 2007	Updated Department of Energy link and references to Form OE-411	Errata

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form OE-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form OE-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form OE-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form OE-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form OE-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.oe.netl.doe.gov/oe417.aspx.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	OE – Sch-1 OE – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	OE – Sch-1 OE – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	OE – Sch-1 OE – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	OE – Sch-1 OE – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	OE – Sch-1 OE – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	OE – Sch-1 OE – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	OE – Sch-1 OE – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	OE – Sch-1 OE – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	OE – Sch-1 OE – Sch-2	1 hour 48 hour
All DOE OE-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE OE-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				
All entities required to file a DOE OE-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day

2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE OE-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE OE-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

A. Introduction

1. **Title:** **System Restoration from Blackstart Resources**

2. **Number:** EOP-005-2

3. **Purpose:** Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators.

   4.2. Generator Operators.

   4.3. Transmission Owners identified in the Transmission Operators restoration plan.

   4.4. Distribution Providers identified in the Transmission Operators restoration plan.

5. **Proposed Effective Date:** Twenty-four months after the first day of the first calendar quarter following applicable regulatory approval. In those jurisdictions where no regulatory approval is required, all requirements go into effect twenty-four months after Board of Trustees adoption.

B. Requirements

R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Violation Risk Factor = High] [Time Horizon = Operations Planning]*

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

R1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

R1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.

R2. Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*

R3. Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

R4. Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R4.1. Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.

R5. Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date. *[Violation Risk Factor = Lower] [Time Horizon = Operations Planning]*

R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify: *[Violation Risk Factor = Medium] [Time Horizon = Long-term Planning]*

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

R7. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration. *[Violation Risk Factor = High] [Time Horizon = Real-time Operations]*

R8. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator. *[Violation Risk Factor = High] [Time Horizon = Real-time Operations]*

R9. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R9.1. The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

R9.2. A list of required tests including:

R9.2.1. The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.

R9.2.2. The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

R9.3. The minimum duration of each of the required tests.

R10. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R10.1. System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.

R10.2. Restoration priorities.

R10.3. Building of cranking paths.

R10.4. Synchronizing (re-energized sections of the System).

R11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R12. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R13. Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R14. Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R15. Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator's restoration plan within 24 hours following such change. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R16. Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R16.1. Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R9.

R16.2. Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.

R17. Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

R17.1. System restoration plan including coordination with the Transmission Operator.

R17.2. The procedures documented in Requirement R14.

R18. Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator. *[Violation Risk Factor = Medium] [Time Horizon = Operations Planning]*

C. Measures

M1. Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator.

M2. Each Transmission Operator shall have evidence such as e-mails with receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan in accordance with Requirement R2.

M3. Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, e-mails with receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.

M4. Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, e-mails with receipts, or registered mail receipts, that it has updated its restoration plan and submitted it to its Reliability Coordinator in accordance with Requirement R4.

M5. Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan available in its primary and backup control rooms and its System Operators prior to its implementation date in accordance with Requirement R5.

M6. Each Transmission Operator shall have documentation such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.

M7. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved shall have evidence such as voice recordings, e-mail, dated computer printouts, or operator logs, that it implemented its restoration plan or restoration plan strategies in accordance with Requirement R7.

M8. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved in such an event shall have evidence, such as voice recordings, e-mail, dated computer printouts, or operator logs, that it resynchronized shut down areas in accordance with Requirement R8.

M9. Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R9.

M10. Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R10.

M11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R11.

M12. Each Transmission Operator shall have evidence, such as training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R12.

M13. Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R13.

M14. Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R14.

M15. Each Generator Operator with a Blackstart Resource shall provide evidence, such as e-mails with receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within twenty-four hours of such changes in accordance with Requirement R15.

M16. Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R16.

M17. Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R17.

M18. Each Generator Operator shall have evidence, such as dated training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R18.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Approved restoration plan and any restoration plans in force since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of an updated restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three years for Requirement R4, Measure M4.
- The current, restoration plan approved by the Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- Implementation of its restoration plan or restoration plan strategies on any occasion for three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R7, Measure M7.
- Resynchronization of shut down areas on any occasion over three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R8, Measure M8.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R9, Measure M9.
- Actual training program materials or descriptions for three calendar years for Requirement R10, Measure M10.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit

as well as one previous compliance audit period for Requirement R12, Measure M12.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator, applicable Transmission Owner, and applicable Distribution provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Actual training program materials or descriptions and actual training records for three calendar years for Requirement R11, Measure M11.

If a Transmission Operator, applicable Transmission owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in force since its last compliance audit for Requirement R13, Measure M13.

The Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current documentation and any documentation in force since its last compliance audit on procedures to start each Blackstart Resources and for energizing a bus for Requirement R14, Measure M14.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R15, Measure M15.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R16, Measure M16.
- Actual training program materials and actual training records for three calendar years for Requirement R17, Measure M17.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Generator Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R18, Measure M18.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Transmission Operator has an approved plan but failed to comply with one of the sub-requirements within the requirement.	The Transmission Operator has an approved plan but failed to comply with two of the sub-requirements within the requirement.	The Transmission Operator has an approved plan but failed to comply with three of the sub-requirements within the requirement.	The Transmission Operator does not have an approved restoration plan.
R2.	The Transmission Operator failed to provide one of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was up to 30 calendar days late in doing so.	The Transmission Operator failed to provide two of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was more than 30 and less than or equal to 60 calendar days late in doing so.	The Transmission Operator failed to provide three of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was more than 60 and less than or equal to 90 calendar days late in doing so.	The Transmission Operator failed to provide four or more of the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. OR The Transmission Operator provided the information to all entities but was more than 90 calendar days late in doing so.
R3.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change within 30 calendar days after the pre-determined schedule.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change more than 30 and less than or equal to 60 calendar days after the pre-determined schedule.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change more than 60 and less than or equal to 90 calendar days after the pre-determined schedule.	The Transmission Operator submitted the reviewed restoration plan or confirmation of no change more than 90 calendar days after the pre-determined schedule.
R4.	The Transmission Operator failed to update and submit its restoration plan to the Reliability Coordinator within 90 calendar days of an unplanned change.	The Transmission Operator failed to update and submit its restoration plan to the Reliability Coordinator within more than 90 calendar days but less than120 calendar days of an unplanned change.	The Transmission Operator has failed to update and submit its restoration plan to the Reliability Coordinator within more than 120 calendar days but less than 150 calendar days of unplanned change.	The Transmission Operator has failed to update and submit its restoration plan to the Reliability Coordinator within more than 150 calendar days of an unplanned change. OR The Transmission Operator failed to update and submit its restoration plan

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				to the Reliability Coordinator prior to a planned BES modification.
R5.	N/A	N/A	N/A	The Transmission Operator did not make the latest Reliability Coordinator approved restoration plan available in its primary and backup control rooms prior to its implementation date.
R6.	The Transmission Operator performed the verification within the required timeframe but did not comply with one of the sub-requirements.	The Transmission Operator performed the verification within the required timeframe but did not comply with two of the sub-requirements.	The Transmission Operator performed the verification but did not complete it within the five calendar year period.	The Transmission Operator did not perform the verification or it took more than six calendar years to complete the verification. OR The Transmission Operator performed the verification within the required timeframe but did not comply with any of the sub-requirements.
R7.	N/A	N/A	N/A	The Transmission Operator did not implement its restoration plan following a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES. Or, if the restoration plan cannot be executed as expected, the Transmission Operator did not utilize its restoration plan strategies to facilitate restoration**.**
R8.	N/A	N/A	N/A	The Transmission Operator resynchronized without approval of the Reliability Coordinator or not in accordance with the established procedures of the Reliability Coordinator following a Disturbance in

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				which Blackstart Resources have been utilized in restoring the shut down area of the BES to service.
R9.	N/A	N/A	N/A	The Transmission Operator's Blackstart Resource testing requirements do not address one or more of the sub-requirements of Requirement R9.
R10.	The Transmission Operator's training does not address one of the sub-requirements of Requirement R10.	The Transmission Operator's training does not address two of the sub-requirements of Requirement R10.	The Transmission Operator's training does not address three or more of the sub-requirements of Requirement R10.	The Transmission Operator has not included System restoration training in its operations training program.
R11.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider did not train less than or equal to 10% of the personnel required by Requirement R11 within a two calendar year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider did not train more than 10% and less than or equal to 25% of the personnel required by Requirement R11 within a two calendar year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider did not train more than 25% and less than or equal to 50% of the personnel required by Requirement R11 within a two calendar year period.	The Transmission Operator, applicable Transmission Owner, or applicable Distribution Provider did not train more than 50 % of the personnel required by Requirement R11 within a two calendar year period.
R12.	N/A.	N/A	N/A	The Transmission Operator has failed to comply with a request for their participation from the Reliability Coordinator.
R13.	N/A	The Transmission Operator and Generator Operator with a Blackstart Resource do not reference Blackstart Resource Testing requirements in their written Blackstart Resource Agreements or mutually agreed upon procedures or protocols.	N/A	The Transmission Operator and Generator Operator with a Blackstart resource do not have a written Blackstart Resource Agreement or mutually agreed upon procedure or protocol.

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R14.	N/A	N/A	N/A	The Generator Operator does not have documented starting and bus energizing procedures for each Blackstart Resource.
R15.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan within 24 hours but did make the notification within 48 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan within 24 hours but did make the notification within 72 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan within 24 hours but did make the notification within 96 hours.	The Generator Operator with a Blackstart Resource did not notify the Transmission Operator of a change in Blackstart Resource capability affecting the ability to meet the Transmission Operator's restoration plan for more than 96 hours.
R16.	The Generator Operator with a Blackstart Resource did not maintain testing records for one of the requirements for a Blackstart Resource. Or did not supply the Blackstart Resource testing records as requested within 59 calendar days of the request.	The Generator Operator with a Blackstart Resource did not maintain testing records for two of the requirements for a Blackstart Resource. Or did not supply the Blackstart Resource testing records as requested for 60 days to 89 calendar days after the request.	The Generator Operator with a Blackstart Resource did not maintain testing records for three of the requirements for a Blackstart Resource. Or did not supply the Blackstart Resource testing records as requested for 90 to 119 calendar days after the request.	The Generator Operator with a Blackstart Resource did not maintain testing records for a Blackstart Resource. Or did not supply the Blackstart Resource testing records as requested for 120 days or more after the request.
R17.	The Generator Operator with a Blackstart Resource did not train less than or equal to 10% of the personnel required by Requirement R17 within a two calendar year period.	The Generator Operator with a Blackstart Resource did not train more than 10% and less than or equal to 25% of the personnel required by Requirement R17 within a two calendar year period.	The Generator Operator with a Blackstart Resource did not train more than 25% and less than or equal to 50% of the personnel required by Requirement R17 within a two calendar year period.	The Generator Operator with a Blackstart Resource did not train more than 50% of the personnel required by Requirement R17 within a two calendar year period.
R18.	N/A.	N/A	N/A	The Generator Operator has failed to comply with a request for their participation from the Reliability Coordinator.

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	May 2, 2007	Approved by Board of Trustees	Revised
2	TBD	Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised

A. Introduction

1. **Title:** **Documentation of Blackstart Generating Unit Test Results**

2. **Number:** EOP-009-0

3. **Purpose:** A system Blackstart Capability Plan (BCP) is necessary to ensure that the quantity and location of system blackstart generators are sufficient and that they can perform their expected functions as specified in overall coordinated Regional System Restoration Plans.

4. **Applicability:**

   4.1. Generator Operator

   4.2. Generator Owner

5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Generator Operator of each blackstart generating unit shall test the startup and operation of each system blackstart generating unit identified in the BCP as required in the Regional BCP (Reliability Standard EOP-007-0_R1). Testing records shall include the dates of the tests, the duration of the tests, and an indication of whether the tests met Regional BCP requirements.

R2. The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

C. Measures

M1. The Generator Operator shall have evidence it provided the test results specified in Reliability Standard EOP-009-0R1 as specified in Reliability Standard EOP-009-0_R2.

D. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Monitoring Responsibility

   Compliance Monitor: Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Timeframe

   Current test results: to the Regional Reliability Organization and upon request to NERC (30 calendar days).

   1.3. Data Retention

   None specified.

   1.4. Additional Compliance Information

   None

2. **Levels of Non-Compliance**

   2.1. Level 1: Startup and operation testing of each blackstart generating unit was performed, but the documentation was incomplete.

   2.2. Level 2: Not applicable.

2.3. Level 3: Startup and operation testing of a blackstart generating unit was only partially performed.

2.4. Level 4: Startup and operation testing of each blackstart generating unit was not performed.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New

A. Introduction

1. **Title:** Coordination of Plans For New Generation, Transmission, and End-User Facilities

2. **Number:** FAC-002-1

3. **Purpose:** To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.

4. **Applicability:**

   4.1. Generator Owner

   4.2. Transmission Owner

   4.3. Distribution Provider

   4.4. Load-Serving Entity

   4.5. Transmission Planner

   4.6. Planning Authority

5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:

1.1. Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.

1.2. Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.

1.3. Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.

1.4. Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.

1.5. Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected

transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

C. Measures

M1. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider's documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.

M2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Timeframe

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting

Complaints

1.4. Data Retention

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

1.5. Additional Compliance Information

None

2. Violation Severity Levels (no changes)

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata
1	TBD	Modified to address Order No. 693 Directives contained in paragraph 693.	Revised.

A. Introduction

1. **Title:** **Facility Ratings Methodology**

2. **Number:** FAC-008-1

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. **Applicability**

   4.1. Transmission Owner

   4.2. Generator Owner

5. **Effective Date:** August 7, 2006

B. Requirements

R1. The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:

R1.1. A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R1.2. The method by which the Rating (of major BES equipment that comprises a Facility) is determined.

R1.2.1. The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

R1.2.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R1.3. Consideration of the following:

R1.3.1. Ratings provided by equipment manufacturers.

R1.3.2. Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).

R1.3.3. Ambient conditions.

R1.3.4. Operating limitations.

R1.3.5. Other assumptions.

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the

Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

C. Measures

M1. The Transmission Owner and Generator Owner shall each have a documented Facility Ratings Methodology that includes all of the items identified in FAC-008 Requirement 1.1 through FAC-008 Requirement 1.3.5.

M2. The Transmission Owner and Generator Owner shall each have evidence it made its Facility Ratings Methodology available for inspection within 15 business days of a request as follows:

M2.1 The Reliability Coordinator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Reliability Coordinator Area.

M2.2 The Transmission Operator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its portion of the Reliability Coordinator Area.

M2.3 The Transmission Planner shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Transmission Planning Area.

M2.4 The Planning Authority shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Planning Authority Area.

M3. If the Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall have evidence that it provided a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Transmission Owner and Generator Owner shall self-certify its compliance to the Compliance Monitor at least once every three years. New Transmission Owners and Generator Owners shall each demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

The Transmission Owner and Generator Owner shall each keep all superseded portions of its Facility Ratings Methodology for 12 months beyond the date of the change in that methodology and shall keep all documented comments on the Facility Ratings Methodology and associated responses for three years. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant.

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Transmission Owner and Generator Owner shall each make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 Facility Ratings Methodology

1.4.2 Superseded portions of its Facility Ratings Methodology that had been replaced, changed or revised within the past 12 months

1.4.3 Documented comments provided by a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Authority on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology, and the associated responses

2. Levels of Non-Compliance

2.1. Level 1: There shall be a level one non-compliance if any of the following conditions exists:

2.1.1 The Facility Ratings Methodology does not contain a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.1.2 The Facility Ratings Methodology does not address one of the required equipment types identified in FAC-008 R1.2.1.

2.1.3 No evidence of responses to a Reliability Coordinator's, Transmission Operator, Transmission Planner, or Planning Authority's comments on the Facility Ratings Methodology.

2.2. Level 2: The Facility Ratings Methodology is missing the assumptions used to determine Facility Ratings or does not address two of the required equipment types identified in FAC-008 R1.2.1.

2.3. Level 3: The Facility Ratings Methodology does not address three of the required equipment types identified in FAC-008-1 R1.2.1.

2.4. Level 4: The Facility Ratings Methodology does not address both Normal and Emergency Ratings or the Facility Ratings Methodology was not made available for inspection within 15 business days of receipt of a request.

E. Regional Differences

None Identified.

Version History

Version	Date	Action	Change Tracking
1	01/01/05	1. Lower cased the word "draft" and "drafting team" where appropriate. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Changed "Timeframe" to "Time	01/20/05

		Frame" and "twelve" to "12" in item D, 1.2.	

A. Introduction

1. **Title:** **Facility Ratings**

2. **Number:** FAC-008-3

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.

4. **Applicability**

   4.1. Transmission Owner.

   4.2. Generator Owner.

5. **Effective Date:** The first day of the first calendar quarter that is twelve months beyond the date approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter twelve months following BOT adoption.

B. Requirements

R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:

- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
- Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:

2.2.1. Equipment Rating standard(s) used in development of this methodology.

2.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

2.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

2.2.4. Operating limitations.[1]

2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.4. The process by which the Rating of equipment that comprises a Facility is determined.

2.4.1. The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

2.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R3. Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

3.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:

3.2.1. Equipment Rating standard(s) used in development of this methodology.

[1] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

3.2.4. Operating limitations.[2]

3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

3.4. The process by which the Rating of equipment that comprises a Facility is determined.

3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R7. Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

[2] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

8.1. As scheduled by the requesting entities:

8.1.1. Facility Ratings

8.1.2. Identity of the most limiting equipment of the Facilities

8.2. Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1. Identity of the existing next most limiting equipment of the Facility

8.2.2. The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

C. Measures

M1. Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.

M2. Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.

M3. Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.

M4. Each Transmission Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement 4. The Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its documentation for determining its Facility Ratings or its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement R4.

M5. If the Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology or a Generator Owner's documentation for determining its Facility Ratings, the Transmission Owner or Generator Owner shall have evidence, (such as a copy of a dated electronic or hard copy note, or other comparable evidence from the Transmission Owner or Generator Owner addressed to the commenter that includes the response to the comment,) that it provided a response to that commenting entity in accordance with Requirement R5.

M6. Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).

M7. Each Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R7.

M8. Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability

Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority**

Regional Entity

1.2. **Compliance Monitoring and Enforcement Processes:**

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting
- Compliance Violation Investigations
- Complaints

1.3. **Data Retention**

The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.

The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.

The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.

The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.

The Generator Owner and Transmission Owner shall each keep evidence for Measure M4, and Measure M5, for three calendar years.

The Generator Owner shall keep evidence for Measure M7 for three calendar years.

The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.

If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. **Additional Compliance Information**

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	• The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part 2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
R3	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	• 3.2.2 • 3.2.3 • 3.2.4	• 3.2.2 • 3.2.3 • 3.2.4	OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
R4	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.	The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.	The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)
R5	The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)	The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)	The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation. (R5)	The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
R7	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the requesting entities.
R8	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)	than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)

E. Regional Variances

None.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	

A. Introduction

1. Title: Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

2. Number: FAC-013-2

3. Purpose: To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.

4. Applicability:

4.1. Planning Coordinators

5. Effective Date:

In those jurisdictions where regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after applicable regulatory approval or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-2 are effective.

In those jurisdictions where no regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after Board of Trustees adoption or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1 and MOD-030-2 are effective.

B. Requirements

R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Criteria for the selection of the transfers to be assessed.

1.2. A statement that the assessment shall respect known System Operating Limits (SOLs).

1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's planning practices.

1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:

1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.

1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.

1.4.3. System demand.

1.4.4. Current approved and projected Transmission uses.

1.4.5. Parallel path (loop flow) adjustments.

1.4.6. Contingencies

1.4.7. Monitored Facilities.

1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.

R2. Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. Distribute to the following prior to the effectiveness of such revisions:

2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.

2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.

2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]*

R4. During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

R5. Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

R6. If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

C. Measures

M1. Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.

M2. Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2

M3. Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3.

M4. Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.

M5. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5.

M6. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Data Retention

The Planning Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment.
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.

R2	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.
R3	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.

R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.

R5	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	08/01/05	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Lower cased the word "draft" and "drafting team" where appropriate. 3. Changed Anticipated Action #5, page 1, from "30-day" to "Thirty-day." 4. Added or removed "periods."	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	5/17/12	FERC Order issued directing the VRF's for Requirements R1. and R4. be changed from "Lower" to "Medium." FERC Order issued correcting the High and Severe VSL language for R1.	

A. Introduction

1. **Title:** **Interchange Confirmation**

2. **Number:** **INT-007-1**

3. **Purpose:** To ensure that each Arranged Interchange is checked for reliability before it is implemented.

4. **Applicability**

   4.1. Interchange Authority.

5. **Effective Date:** January 1, 2007

B. Requirements

R1. The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:

R1.1. Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

R1.3. The following are defined:

R1.3.1. Generation source and load sink.

R1.3.2. Megawatt profile.

R1.3.3. Ramp start and stop times.

R1.3.4. Interchange duration.

R1.4. Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.

C. Measures

M1. For each Arranged Interchange, the Interchange Authority shall show evidence that it has verified the Arranged Interchange information prior to the dissemination of the Confirmed Interchange.

D. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Monitoring Responsibility

   Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Time Frame

   The Performance-Reset Period shall be twelve months from the last noncompliance to Requirement 1.

   1.3. Data Retention

   The Interchange Authority shall keep 90 days of historical data. The Compliance Monitor shall keep audit records for a minimum of three calendar years.

1.4. Additional Compliance Information

Each Interchange Authority shall demonstrate compliance to the Compliance Monitor within the first year that this standard becomes effective or the first year the entity commences operation by self-certification to the Compliance Monitor.

Subsequent to the initial compliance review, compliance may be:

1.4.1 Verified by audit at least once every three years.

1.4.2 Verified by spot checks in years between audits.

1.4.3 Verified by annual audits of noncompliant Interchange Authorities, until compliance is demonstrated.

1.4.4 Verified at any time as the result of a complaint. Complaints must be lodged within 60 days of the incident. Complaints will be evaluated by the Compliance Monitor.

Each Interchange Authority shall make the following available for inspection by the Compliance Monitor upon request:

1.4.5 For compliance audits and spot checks, relevant data and system log records for the audit period which indicate an Interchange Authority's verification that all Arranged Interchange was balanced and valid as defined in R1. The Compliance Monitor may request up to a three-month period of historical data ending with the date the request is received by the Interchange Authority.

1.4.6 For specific complaints, only those data and system log records associated with the specific Interchange event contained in the complaint which indicate an Interchange Authority's verification that an Arranged Interchange was balanced and valid as defined in R1 for that specific Interchange

2. Levels of Non-Compliance

2.1. Level 1: One occurrence[1] where Interchange-related data was not verified as defined in R1.

2.2. Level 2: Two occurrences where Interchange-related data was not verified as defined in R1.

2.3. Level 3: Three occurrences where Interchange-related data was not verified as defined in R1.

2.4. Level 4: Four or more occurrences where Interchange-related data was not verified as defined in R1.

E. Regional Differences

None

[1] This does not include instances of not verifying due to extenuating circumstances approved by the Compliance Monitor.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. **Title:** **Coordination of Real-time Activities Between Reliability Coordinators**

2. **Number:** **IRO-016-1**

3. **Purpose:** To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.

4. **Applicability**

   4.1. Reliability Coordinator

5. **Effective Date:** November 1, 2006

B. Requirements

R1. The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.

R1.1. If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.

R1.2. If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).

R1.2.1. If time permits, this re-evaluation shall be done before taking corrective actions.

R1.2.2. If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

R1.3. If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

C. Measures

M1. For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

D. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Monitoring Responsibility

   Regional Reliability Organization

   1.2. Compliance Monitoring Period and Reset Time Frame

   The performance reset period shall be one calendar year.

1.3. Data Retention

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

1.4. Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction's discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

2. Levels of Non-Compliance

2.1. Level 1: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
Version 1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Hyphenated "30-day" and "Reliability Coordinator-to-Reliability Coordinator" when used as adjective.	01/20/06

		3. Changed standard header to be consistent with standard "Title." 4. Added "periods" to items where appropriate. 5. Initial capped heading "Definitions of Terms Used in Standard." 6. Changed "Timeframe" to "Time Frame" in item D, 1.2. 7. Lower cased all words that are not "defined" terms — drafting team, and self-certification. 8. Changed apostrophes to "smart" symbols. 9. Removed comma after word "condition" in item R.1.1. 10. Added comma after word "expected" in item 1.4, last sentence. 11. Removed extra spaces between words where appropriate.	

A. Introduction

1. **Title:** **Capacity Benefit Margin**

2. **Number:** **MOD-004-1**

3. **Purpose:** To promote the consistent and reliable calculation, verification, preservation, and use of Capacity Benefit Margin (CBM) to support analysis and system operations.

4. **Applicability:**

   4.1. Load-Serving Entities.

   4.2. Resource Planners.

   4.3. Transmission Service Providers.

   4.4. Balancing Authorities.

   4.5. Transmission Planners, when their associated Transmission Service Provider has elected to maintain CBM.

5. **Effective Date:** First day of the first calendar quarter that is twelve months beyond the date that this standard is approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the standard becomes effective on the first day of the first calendar quarter that is twelve months beyond the date this standard is approved by the NERC Board of Trustees.

B. Requirements

R1. The Transmission Service Provider that maintains CBM shall prepare and keep current a "Capacity Benefit Margin Implementation Document" (CBMID) that includes, at a minimum, the following information: [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning, Long-term Planning*]

R1.1. The process through which a Load-Serving Entity within a Balancing Authority Area associated with the Transmission Service Provider, or the Resource Planner associated with that Balancing Authority Area, may ensure that its need for Transmission capacity to be set aside as CBM will be reviewed and accommodated by the Transmission Service Provider to the extent Transmission capacity is available.

R1.2. The procedure and assumptions for establishing CBM for each Available Transfer Capability (ATC) Path or Flowgate.

R1.3. The procedure for a Load-Serving Entity or Balancing Authority to use Transmission capacity set aside as CBM, including the manner in which the Transmission Service Provider will manage situations where the requested use of CBM exceeds the amount of CBM available.

R2. The Transmission Service Provider that maintains CBM shall make available its current CBMID to the Transmission Operators, Transmission Service Providers, Reliability Coordinators, Transmission Planners, Resource Planners, and Planning Coordinators that are within or adjacent to the Transmission Service Provider's area, and to the Load Serving Entities and Balancing Authorities within the Transmission Service Provider's

area, and notify those entities of any changes to the CBMID prior to the effective date of the change. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]

R3. Each Load-Serving Entity determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by: [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]

R3.1. Using one or more of the following to determine the GCIR:

- Loss of Load Expectation (LOLE) studies
- Loss of Load Probability (LOLP) studies
- Deterministic risk-analysis studies
- Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities

R3.2. Identifying expected import path(s) or source region(s).

R4. Each Resource Planner determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by: [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]

R4.1. Using one or more of the following to determine the GCIR:

- Loss of Load Expectation (LOLE) studies
- Loss of Load Probability (LOLP) studies
- Deterministic risk-analysis studies
- Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities

R4.2. Identifying expected import path(s) or source region(s).

R5. At least every 13 months, the Transmission Service Provider that maintains CBM shall establish a CBM value for each ATC Path or Flowgate to be used for ATC or Available Flowgate Capability (AFC) calculations during the 13 full calendar months (months 2-14) following the current month (the month in which the Transmission Service Provider is establishing the CBM values). This value shall: [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]

R5.1. Reflect consideration of each of the following if available:

- Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Service Provider's area
- Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Service Provider's area

- Any reserve margin or resource adequacy requirements for loads within the Transmission Service Provider's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities

R5.2. Be allocated as follows:

- For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners
- For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Service Provider

R6. At least every 13 months, the Transmission Planner shall establish a CBM value for each ATC Path or Flowgate to be used in planning during each of the full calendar years two through ten following the current year (the year in which the Transmission Planner is establishing the CBM values). This value shall: [*Violation Risk Factor: Lower*] [*Time Horizon: Long-term Planning*]

R6.1. Reflect consideration of each of the following if available:

- Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Planner's area
- Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Planner's area
- Any reserve margin or resource adequacy requirements for loads within the Transmission Planner's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities

R6.2. Be allocated as follows:

- For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners
- For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Planner.

R7. Less than 31 calendar days after the establishment of CBM, the Transmission Service Provider that maintains CBM shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the Transmission Service Provider's system of the amount of CBM set aside. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]

R8. Less than 31 calendar days after the establishment of CBM, the Transmission Planner shall notify all the Load-Serving Entities and Resource Planners that determined they

had a need for CBM on the system being planned by the Transmission Planner of the amount of CBM set aside. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*]

R9. The Transmission Service Provider that maintains CBM and the Transmission Planner shall each provide (subject to confidentiality and security requirements) copies of the applicable supporting data, including any models, used for determining CBM or allocating CBM over each ATC Path or Flowgate to the following: [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning, Long-term Planning*]

R9.1. Each of its associated Transmission Operators within 30 calendar days of their making a request for the data.

R9.2. To any Transmission Service Provider, Reliability Coordinator, Transmission Planner, Resource Planner, or Planning Coordinator within 30 calendar days of their making a request for the data.

R10. The Load-Serving Entity or Balancing Authority shall request to import energy over firm Transfer Capability set aside as CBM only when experiencing a declared NERC Energy Emergency Alert (EEA) 2 or higher. [*Violation Risk Factor: Lower*] [*Time Horizon: Same-day Operations*]

R11. When reviewing an Arranged Interchange using CBM, all Balancing Authorities and Transmission Service Providers shall waive, within the bounds of reliable operation, any Real-time timing and ramping requirements. [*Violation Risk Factor: Medium*] [*Time Horizon: Same-day Operations*]

R12. The Transmission Service Provider that maintains CBM shall approve, within the bounds of reliable operation, any Arranged Interchange using CBM that is submitted by an "energy deficient entity[1]" under an EEA 2 if: [*Violation Risk Factor: Medium*] [*Time Horizon: Same-day Operations*]

R12.1. The CBM is available

R12.2. The EEA 2 is declared within the Balancing Authority Area of the "energy deficient entity," and

R12.3. The Load of the "energy deficient entity" is located within the Transmission Service Provider's area.

C. Measures

M1. Each Transmission Service Provider that maintains CBM shall produce its CBMID evidencing inclusion of all information specified in R1. (R1)

M2. Each Transmission Service Provider that maintains CBM shall have evidence (such as dated logs and data, copies of dated electronic messages, or other equivalent evidence) to show that it made the current CBMID available to the Transmission Operators, Transmission Service Providers, Reliability Coordinators, Transmission Planners, and Planning Coordinators specified in R2, and that prior to any change to the CBMID, it notified those entities of the change. (R2)

[1] See Attachment 1-EOP-002-0 for explanation.

M3. Each Load-Serving Entity that determined a need for Transmission capacity to be set aside as CBM shall provide evidence (including studies and/or requirements) that it met the criteria in R3. (R3)

M4. Each Resource Planner that determined a need for Transmission capacity to be set aside as CBM shall provide evidence (including studies and/or requirements) that it met the criteria in R4. (R4)

M5. Each Transmission Service Provider that maintains CBM shall provide evidence (such as studies, requirements, and dated CBM values) that it established 13 months of CBM values consistent with the requirements in R5.1 and allocated the values consistent with the requirements in R5.2. (Note that CBM values may legitimately be zero.) (R5)

M6. Each Transmission Planner with an associated Transmission Service Provider that maintains CBM shall provide evidence (such as studies, requirements, and dated CBM values) that it established CBM values for years two through ten consistent with the requirements in R6.1 and allocated the values consistent with the requirements in R6.2. Inclusion of GCIR based on R6.1 and R6.2 within the transmission base case meets this requirement. (Note that CBM values may legitimately be zero.) (R6)

M7. Each Transmission Service Provider that maintains CBM shall provide evidence (such as dated e-mail, data, or other records) that it notified the entities described in R7 of the amount of CBM set aside. (R7)

M8. Each Transmission Planner with an associated Transmission Service Provider that maintains CBM shall provide evidence (such as e-mail, data, or other records) that it notified the entities described in R8 of the amount of CBM set aside. (R8)

M9. Each Transmission Service Provider that maintains CBM and each Transmission Planner shall provide evidence including copies of dated requests for data supporting the calculation of CBM along with other evidences such as copies of electronic messages or other evidence to show that it provided the required entities with copies of the supporting data, including any models, used for allocating CBM as specified in R9. (R9)

M10. Each Load-Serving Entity and Balancing Authority shall provide evidence (such as logs, copies of tag data, or other data from its Reliability Coordinator) that at the time it requested to import energy using firm Transfer Capability set aside as CBM, it was in an EEA 2 or higher. (R10)

M11. Each Balancing Authority and Transmission Service Provider shall provide evidence (such as operating logs and tag data) that it waived Real-time timing and ramping requirements when approving an Arranged Interchange using CBM (R11)

M12. Each Transmission Service Provider that maintains CBM shall provide evidence including copies of CBM values along with other evidence (such as tags, reports, and supporting data) to show that it approved any Arranged Interchange meeting the criteria in R12. (R12)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority (CEA)

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Data Retention

- The Transmission Service Provider that maintains CBM shall maintain its current, in force CBMID and any prior versions of the CBMID that were in force during the past three calendar years plus the current year to show compliance with R1.
- The Transmission Service Provider that maintains CBM shall maintain evidence to show compliance with R2, R5, R7, R9, and R12 for the most recent three calendar years plus the current year.
- The Load-Serving Entity shall each maintain evidence to show compliance with R3 and R10 for the most recent three calendar years plus the current year.
- The Resource Planner shall each maintain evidence to show compliance with R4 for the most recent three calendar years plus the current year.
- The Transmission Planner shall maintain evidence to show compliance with R6, R8, and R9 for the most recent three calendar years plus the current year.
- The Balancing Authority shall maintain evidence to show compliance with R10 and R11 for the most recent three calendar years plus the current year.
- The Transmission Service Provider shall maintain evidence to show compliance with R11 for the most recent three calendar years plus the current year.
- If an entity is found non-compliant, it shall keep information related to the non-compliance until found compliant.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and subsequently submitted audit records.

1.4. Compliance Monitoring and Enforcement Processes:

The following processes may be used:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting

- Complaints

1.5. Additional Compliance Information

None.

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Transmission Service Provider that maintains CBM has a CBMID that does not incorporate changes that have been made within the last three months.	The Transmission Service Provider that maintains CBM has a CBMID that does not incorporate changes that have been made more than three, but not more than six, months ago. **OR** The CBM maintaining Transmission Service Provider's CBMID does not address one of the sub requirements.	The Transmission Service Provider that maintains CBM has a CBMID that does not incorporate changes that have been made more than six, but not more than twelve, months ago. **OR** The CBM maintaining Transmission Service Provider's CBMID does not address two of the sub requirements.	The Transmission Service Provider that maintains CBM has a CBMID that does not incorporate changes that have been made more than twelve months ago. **OR** The Transmission Service Provider that maintains CBM does not have a CBMID; **OR** The CBM maintaining Transmission Service Provider's CBMID does not address three of the sub requirements.
R2.	The Transmission Service Provider that maintains CBM notifies one or more of the entities specified in R2 of a change in the CBM ID after the effective date of the change, but not more than 30 calendar days after the effective date of the change.	The Transmission Service Provider that maintains CBM notifies one or more of the entities specified in R2 of a change in the CBM ID 30 or more calendar days but not more than 60 calendar days after the effective date of the change.	The Transmission Service Provider that maintains CBM notifies one or more of the entities specified in R2 of a change in the CBM ID 60 or more calendar days but not more than 90 calendar days after the effective date of the change. **OR** The Transmission Service Provider that maintains CBM made available the CBMID to at least one, but not all, of the entities specified in R2.	The Transmission Service Provider that maintains CBM notifies one or more of the entities specified in R2 of a change in the CBM ID more than 90 calendar days after the effective date of the change. **OR** The Transmission Service Provider that maintains CBM made available the CBMID to none of the entities specified in R2.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.		The Load-Serving Entity did not use one of the methods described in R3.1 **OR** The Load-Serving Entity did not identify paths or regions as described in R3.2		The Load-Serving Entity did not use one of the methods described in R3.1 **AND** The Load-Serving Entity did not identify paths or regions as described in R3.2
R4		The Resource Planner did not use one of the methods described in R4.1 **OR** The Resource Planner did not identify paths or regions as described in R4.2		The Resource Planner did not use one of the methods described in R4.1 **AND** The Resource Planner did not identify paths or regions as described in R4.2
R5.	The Transmission Service Provider that maintains CBM established CBM more than 13 months, but not more than 16 months, after the last time the values were established.	The Transmission Service Provider that maintains CBM established CBM more than 16 months, but not more than 19 months, after the last time the values were established. **OR** The Transmission Service Provider that maintains CBM did not consider one or more of the items described in R5.1 that was available. **OR** The Transmission Service Provider that maintains CBM did not base the allocation on one or more paths or regions as	The Transmission Service Provider that maintains CBM established CBM more than 19 months, but not more than 22 months, after the last time the values were established.	The Transmission Service Provider that maintains CBM established CBM more than 22 months after the last time the values were established. **OR** The Transmission Service Provider that maintains CBM failed to establish an initial value for CBM. **OR** The Transmission Service Provider that maintains CBM did not consider one or more of the items described in R5.1 that was available, and did not base the allocation on one or more

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
		described in R5.2.		paths or regions as described in R5.2
R6.	The Transmission Planner with an associated Transmission Service Provider that maintains CBM established CBM for each of the years 2 through 10 more than 13 months, but not more than 16 months, after the last time the values were established.	The Transmission Planner with an associated Transmission Service Provider that maintains CBM established CBM for each of the years 2 through 10 more than 16 months, but not more than 19 months, after the last time the values were established. **OR** The Transmission Planner with an associated Transmission Service Provider that maintains CBM did not consider one or more of the items described in R6.1 that was available. **OR** The Transmission Planner with an associated Transmission Service Provider that maintains CBM did not base the allocation	The Transmission Planner with an associated Transmission Service Provider that maintains CBM established CBM for each of the years 2 through 10 more than 19 months, but not more than 22 months, after the last time the values were established.	The Transmission Planner with an associated Transmission Service Provider that maintains CBM established CBM for each of the years 2 through 10 more than 22 months after the last time the values were established. **OR** The Transmission Planner with an associated Transmission Service Provider that maintains CBM failed to establish an initial value for CBM for each of the years 2 through 10. **OR** The Transmission Planner with an associated Transmission Service Provider that maintains CBM did not consider one or more of the items described in

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
		on one or more paths or regions as described in R6.2		R6.1 that was available, and did not base the allocation on one or more paths or regions as described in R6.2
R7.	The Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 31 or more days, but less than 45 days.	The Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 45 or more days, but less than 60 days.	The Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 60 or more days, but less than 75 days. **OR** The Transmission Service Provider that maintains CBM notified at least one, but not all, of the entities as required.	The Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 75 or more days, **OR** The Transmission Service Provider that maintains CBM notified none of the entities as required.
R8.	The Transmission Planner with an associated Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 31 or more days, but less than 45 days.	The Transmission Planner with an associated Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 45 or more days, but less than 60 days.	The Transmission Planner with an associated Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 60 or more days, but less than 75 days. **OR** The Transmission Planner with	The Transmission Planner with an associated Transmission Service Provider that maintains CBM notified all the entities as required, but did so in 75 or more days, **OR** The Transmission Planner with an associated Transmission

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
			an associated Transmission Service Provider that maintains CBM notified at least one, but not all, of the entities as required.	Service Provider that maintains CBM notified none of the entities as required.
R9.	The Transmission Service Provider or Transmission Planner provided a requester specified in R9 with the supporting data, including models, used to allocate CBM more than 30, but not more than 45, days after the submission of the request.	The Transmission Service Provider or Transmission Planner provided a requester specified in R9 with the supporting data, including models, used to allocate CBM more than 45, but not more than 60, days after the submission of the request.	The Transmission Service Provider or Transmission Planner provided a requester specified in R9 with the supporting data, including models, used to allocate CBM more than 60, but not more than 75, days after the submission of the request. **OR** The Transmission Service Provider or Transmission Planner provided at least one, but not all, of the requesters specified in R9 with the supporting data, including models, used to allocate CBM.	The Transmission Service Provider or Transmission Planner provided a requester specified in R9 with the supporting data, including models, used to allocate CBM more than 75 days after the submission of the request. **OR** The Transmission Service Provider or Transmission Planner provided none of the requesters specified in R9 with the supporting data, including models, used to allocate CBM.
R10.	N/A	N/A	N/A	A Load-Serving Entity or Balancing Authority requested to schedule energy over CBM while not in an EEA 2 or higher.
R11.	N/A	N/A	N/A	A Balancing Authority or Transmission Service Provider denied an Arranged Interchange using CBM based on timing or ramping requirements without a reliability reason to do so.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R12.	N/A	N/A	N/A	The Transmission Service Provider failed to approve an Arranged Interchange for CBM that met the criteria described in R12 without a reliability reason to do so.

A. Introduction

1. Title: **Nuclear Plant Interface Coordination**

2. Number: NUC-001-2

3. Purpose: This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. Applicability:

4.1. Nuclear Plant Generator Operator.

4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

4.2.1 Transmission Operators.

4.2.2 Transmission Owners.

4.2.3 Transmission Planners.

4.2.4 Transmission Service Providers.

4.2.5 Balancing Authorities.

4.2.6 Reliability Coordinators.

4.2.7 Planning Coordinators.

4.2.8 Distribution Providers.

4.2.9 Load-serving Entities.

4.2.10 Generator Owners.

4.2.11 Generator Operators.

5. Effective Date: April 1, 2010

B. Requirements

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Medium*]

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

R4.1. Incorporate the NPIRs into their operating analyses of the electric system.

R4.2. Operate the electric system to meet the NPIRs.

R4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

R5. The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement.

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3. A requirement to review the agreement(s) at least every three years.

R9.1.4. A dispute resolution mechanism.

R9.2. Technical requirements and analysis:

R9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

R9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

R9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

R9.3. Operations and maintenance coordination:

R9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

R9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

R9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

R9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

R9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. .

R9.3.6. Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

R9.3.7. Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

R9.4. Communications and training:

R9.4.1. Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

R9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

R9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

R9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

R9.4.5. Provisions for personnel training, as related to NPIRs.

C. Measures

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. (Requirement 2 and 9)

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:

M4.1 The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)

M4.2 The electric system was operated to meet the NPIRs. (Requirement 4.2)

M4.3 The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)

M8. The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.

- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

2.1. Lower: Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.

2.2. Moderate: Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.

2.3. High: One or more requirements of R3 through R8 were not met.

2.4. Severe: No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

E. Regional Differences

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs.
Therefore the definition of NPLR for Canadian CANDU units will be as follows:

Nuclear Plant Licensing Requirements (NPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5	Revision

		and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update

A. Introduction

1. **Title:** **Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program**

2. **Number:** PRC-008-0

3. **Purpose:** Provide last resort system preservation measures by implementing an Under Frequency Load Shedding (UFLS) program.

4. **Applicability:**

   4.1. Transmission Owner required by its Regional Reliability Organization to have a UFLS program

   4.2. Distribution Provider required by its Regional Reliability Organization to have a UFLS program

5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.

R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).

C. Measures

M1. Each Transmission Owner's and Distribution Provider's UFLS equipment maintenance and testing program contains the elements specified in Reliability Standard PRC-008-0_R1.

M2. Each Transmission Owner and Distribution Provider shall have evidence that it provided the results of its UFLS equipment maintenance and testing program's implementation to its Regional Reliability Organization and NERC on request (within 30 calendar days).

D. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Monitoring Responsibility

   Compliance Monitor: Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Timeframe

   On request (within 30 calendar days).

   1.3. Data Retention

   None specified.

   1.4. Additional Compliance Information

   None.

2. Levels of Non-Compliance

2.1. Level 1: Documentation of the maintenance and testing program was incomplete, but records indicate implementation was on schedule.

2.2. Level 2: Complete documentation of the maintenance and testing program was provided, but records indicate that implementation was not on schedule.

2.3. Level 3: Documentation of the maintenance and testing program was incomplete, and records indicate implementation was not on schedule.

2.4. Level 4: Documentation of the maintenance and testing program, or its implementation was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	September 26, 2005	Fixed reference in M1 from PRC-007-0_R1 to PRC-008-0_R1.	Errata

A. Introduction

1. **Title:** **Analysis and Documentation of Underfrequency Load Shedding Performance Following an Underfrequency Event**

2. **Number:** PRC-009-0

3. **Purpose:** Provide last resort System preservation measures by implementing an Under Frequency Load Shedding (UFLS) program.

4. **Applicability:**

   4.1. Transmission Owner required by its Regional Reliability Organization to own a UFLS program

   4.2. Transmission Operator required by its Regional Reliability Organization to operate a UFLS program

   4.3. Load-Serving Entity required by the Regional Reliability Organization to operate a UFLS program

   4.4. Distribution Provider required by the Regional Reliability Organization to own or operate a UFLS program

5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UFLS set points and tripping times.

R1.3. A simulation of the event.

R1.4. A summary of the findings.

R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.

C. Measures

M1. Each Transmission Owner's, Transmission Operator's, Load-Serving Entity's and Distribution Provider's documentation of the UFLS program performance following an underfrequency event includes all elements identified in Reliability Standard PRC-009-0_R1.

M2. Each Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operate a UFLS program, shall have evidence it provided documentation of the analysis of the UFLS program performance following an underfrequency event as specified in Reliability Standard PRC-009-0_R1.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

On request 90 calendar days after the system event.

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Analysis of UFLS program performance following an actual underfrequency event below the UFLS set point(s) was incomplete in one or more elements in Reliability Standard PRC-009-0_R1.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: Analysis of UFLS program performance following an actual underfrequency event below the UFLS set point(s) was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New

A. Introduction

1. **Title:** **Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.**

2. **Number:** PRC-010-0

3. **Purpose:** Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.

4. **Applicability:**

   4.1. Load-Serving Entity that operates a UVLS program

   4.2. Transmission Owner that owns a UVLS program

   4.3. Transmission Operator that operates a UVLS program

   4.4. Distribution Provider that owns or operates a UVLS program

5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).

R1.1. This assessment shall include, but is not limited to:

R1.1.1. Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.

R1.1.2. Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.

R1.1.3. A review of the voltage set points and timing.

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

C. Measures

M1. Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0_R1.

M2. Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0_R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

1.2. Compliance Monitoring Period and Reset Timeframe

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0_R1.1 or an assessment of the UVLS program was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New

A. Introduction

1. **Title:** **Under-Voltage Load Shedding Program Performance**

2. **Number:** **PRC-022-1**

3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).

4. **Applicability**

   4.1. Transmission Operator that operates a UVLS program.

   4.2. Distribution Provider that operates a UVLS program.

   4.3. Load-Serving Entity that operates a UVLS program.

5. **Effective Date:** May 1, 2006

B. Requirements

R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UVLS set points and tripping times.

R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.

R1.4. A summary of the findings.

R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

C. Measures

M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.

M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization.

D. Compliance

1. Compliance Monitoring Process

   1.1. Compliance Monitoring Responsibility

   Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

2.3. Level 3: Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

2.4. Level 4: Documentation of the analysis of UVLS performance was not provided.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	12/01/05	1. Removed comma after 2004 in "Development Steps Completed," #1. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Lower cased the word "region," "board," and "regional" throughout document where appropriate. 4. Added or removed "periods" where appropriate. 5. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/06

A. Introduction

1. Title: **Reliability Responsibilities and Authorities**

2. Number: TOP-001-1a

Purpose: To ensure reliability entities have clear decision-making authority and capabilities to take appropriate actions or direct the actions of others to return the transmission system to normal conditions during an emergency.

3. Applicability

3.1. Balancing Authorities

3.2. Transmission Operators

3.3. Generator Operators

3.4. Distribution Providers

3.5. Load Serving Entities

4. Effective Date: Immediately after approval of applicable regulatory authorities.

B. Requirements

R1. Each Transmission Operator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area and shall exercise specific authority to alleviate operating emergencies.

R2. Each Transmission Operator shall take immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.

R3. Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.

R4. Each Distribution Provider and Load Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions.

R5. Each Transmission Operator shall inform its Reliability Coordinator and any other potentially affected Transmission Operators of real time or anticipated emergency conditions, and take actions to avoid, when possible, or mitigate the emergency.

R6. Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.

R7. Each Transmission Operator and Generator Operator shall not remove Bulk Electric System facilities from service if removing those facilities would burden neighboring systems unless:

R7.1. For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.

R7.2. For a transmission facility, the Transmission Operator shall notify and coordinate with its Reliability Coordinator. The Transmission Operator shall notify other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.

R7.3. When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.

R8. During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.

C. Measures

M1. Each Transmission Operator shall have and provide upon request evidence that could include, but is not limited to, signed agreements, an authority letter signed by an officer of the company, or other equivalent evidence that will be used to confirm that it has the authority, and has exercised the authority, to alleviate operating emergencies as described in Requirement 1.

M2. If an operating emergency occurs the Transmission Operator that experienced the emergency shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to determine if it took immediate actions to alleviate the operating emergency including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc. (Requirement 2)

M3. Each Transmission Operator, Balancing Authority, and Generator Operator shall have and provide upon request evidence such as operator logs, voice recordings or

transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to determine if it complied with its Reliability Coordinator's reliability directives. If the Transmission Operator, Balancing Authority or Generator Operator did not comply with the directive because it would violate safety, equipment, regulatory or statutory requirements, it shall provide evidence such as operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that it immediately informed the Reliability Coordinator of its inability to perform the directive. (Requirement 3)

M4. Each Balancing Authority, Generator Operator, Distribution Provider and Load Serving Entity shall have and provide upon request evidence such as operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to determine if it complied with its Transmission Operator's reliability directives. If the Balancing Authority, Generator Operator, Distribution Provider and Load Serving Entity did not comply with the directive because it would violate safety, equipment, regulatory or statutory requirements, it shall provide evidence such as operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that it immediately informed the Transmission Operator of its inability to perform the directive. (Requirements 3 and 4)

M5. The Transmission Operator shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to determine if it informed its Reliability Coordinator and any other potentially affected Transmission Operators of real time or anticipated emergency conditions, and took actions to avoid, when possible, or to mitigate an emergency. (Requirement 5)

M6. The Transmission Operator, Balancing Authority, and Generator Operator shall each have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to determine if it rendered assistance to others as requested, provided that the requesting entity had implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements. (Requirement 6)

M7. The Transmission Operator and Generator Operator shall each have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to determine if it notified either their Transmission Operator in the case of the Generator Operator, or other Transmission Operators, and the Reliability Coordinator when it removed Bulk Electric System facilities from service if removing those facilities would burden neighboring systems. (Requirement 7)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Transmission Operator shall have the current in-force document to show that it has the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area. (Measure 1)

Each Transmission Operator shall keep 90 days of historical data (evidence) for Measures 1 through 7, including evidence of directives issued for Measures 3 and 4.

Each Balancing Authority shall keep 90 days of historical data (evidence) for Measures 3, 4 and 6 including evidence of directives issued for Measures 3 and 4.

Each Generator Operator shall keep 90 days of historical data (evidence) for Measures 3, 4, 6 and 7 including evidence of directives issued for Measures 3 and 4.

Each Distribution Provider and Load-serving Entity shall keep 90 days of historical data (evidence) for Measure 4.

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all supporting compliance data

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance for a Balancing Authority:

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: There shall be a separate Level 4 non-compliance, for every one of the following requirements that is in violation:

2.4.1 Did not comply with a Reliability Coordinator's or Transmission Operator's reliability directive or did not immediately inform the Reliability Coordinator or Transmission Operator of its inability to perform that directive (R3)

2.4.2 Did not render emergency assistance to others as requested, in accordance with R6.

3. Levels of Non-Compliance for a Transmission Operator

3.1. Level 1: Not applicable.

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable.

3.4. Level 4: There shall be a separate Level 4 non-compliance, for every one of the following requirements that is in violation:

3.4.1 Does not have the documented authority to act as specified in R1.

3.4.2 Does not have evidence it acted with the authority specified in R1.

3.4.3 Did not take immediate actions to alleviate operating emergencies as specified in R2.

3.4.4 Did not comply with its Reliability Coordinator's reliability directive or did not immediately inform the Reliability Coordinator of its inability to perform that directive, as specified in R3.

3.4.5 Did not inform its Reliability Coordinator and other potentially affected Transmission Operators of real time or anticipated emergency conditions as specified in R5.

3.4.6 Did not take actions to avoid, when possible, or to mitigate an emergency as specified in R5.

3.4.7 Did not render emergency assistance to others as requested, as specified in R6.

3.4.8 Removed Bulk Electric System facilities from service under conditions other than those specified in R7.1, 7.2, and 7.3, and removing those facilities burdened a neighbor system.

4. Levels of Non-Compliance for a Generator Operator:

4.1. Level 1: Not applicable.

4.2. Level 2: Not applicable.

4.3. Level 3: Not applicable.

4.4. Level 4: There shall be a separate Level 4 non-compliance, for every one of the following requirements that is in violation:

4.4.1 Did not comply with a Reliability Coordinator or Transmission Operator's reliability directive or did not immediately inform the Reliability Coordinator or Transmission Operator of its inability to perform that directive, as specified in R3.

4.4.2 Did not render all available emergency assistance to others as requested, unless such actions would violate safety, equipment, or regulatory or statutory requirements as specified in R6.

4.4.3 Removed Bulk Electric System facilities from service under conditions other than those specified in R7.1, 7.2, and 7.3, and burdened a neighbor system.

5. Levels of Non-Compliance for a Distribution Provider or Load Serving Entity

5.1. Level 1: Not applicable.

5.2. Level 2: Not applicable.

5.3. Level 3: Not applicable

5.4. Level 4: Did not comply with a Transmission Operator's reliability directive or immediately inform the Transmission Operator of its inability to perform that directive, as specified in R4.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1a	May 12, 2010	Added Appendix 1 – Interpretation of R8 approved by BOT on May 12, 2010	Interpretation
1a	September 15, 2011	FERC Order issued approved the Interpretation of R8 (FERC Order became effective November 21, 2011)	Interpretation

Appendix 1

Requirement Number and Text of Requirement
R8. During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.
Question
For Requirement R8 is the Balancing Authority responsibility to immediately take corrective action to restore Real Power Balance and is the TOP responsibility to immediately take corrective action to restore Reactive Power Balance?
Response
The answer to both questions is yes. According to the NERC *Glossary of Terms Used in Reliability Standards*, the Transmission Operator is responsible for the reliability of its "local" transmission system, and operates or directs the operations of the transmission facilities. Similarly, the Balancing Authority is responsible for maintaining load-interchange-generation balance, i.e., real power balance. In the context of this requirement, the Transmission Operator is the functional entity that balances reactive power. Reactive power balancing can be accomplished by issuing instructions to the Balancing Authority or Generator Operators to alter reactive power injection. Based on NERC Reliability Standard BAL-005-1b Requirement R6, the Transmission Operator has no requirement to compute an Area Control Error (ACE) signal or to balance real power. Based on NERC Reliability Standard VAR-001-1 Requirement R8, the Balancing Authority is not required to resolve reactive power balance issues. According to TOP-001-1 Requirement R3, the Balancing Authority is only required to comply with Transmission Operator or Reliability Coordinator instructions to change injections of reactive power.

A. Introduction

1. Title: **Operational Reliability Information**

2. Number: TOP-005-2a

3. Purpose: To ensure reliability entities have the operating data needed to monitor system conditions within their areas.

4. Applicability

4.1. Transmission Operators.

4.2. Balancing Authorities.

4.3. Purchasing Selling Entities.

5. Proposed Effective Date: In those jurisdictions where no regulatory approval is required, the standard shall become effective on the latter of either April 1, 2009 or the first day of the first calendar quarter, three months after BOT adoption.

In those jurisdictions where regulatory approval is required, the standard shall become effective on the latter of either April 1, 2009 or the first day of the first calendar quarter, three months after applicable regulatory approval.

B. Requirements

R1. As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."

R2. Upon request, each Balancing Authority and Transmission Operator shall provide to other Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability, the operating data that are necessary to allow these Balancing Authorities and Transmission Operators to perform operational reliability assessments and to coordinate reliable operations. Balancing Authorities and Transmission Operators shall provide the types of data as listed in Attachment 1-TOP-005 "Electric System Reliability Data," unless otherwise agreed to by the Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability.

R3. Each Purchasing-Selling Entity shall provide information as requested by its Host Balancing Authorities and Transmission Operators to enable them to conduct operational reliability assessments and coordinate reliable operations.

C. Measures

M1. Evidence that the Balancing Authority, Transmission Operator, and Purchasing-Selling Entity is providing the information required, within the time intervals specified, and in a format agreed upon by the requesting entities.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Self-Certification: Entities shall annually self-certify compliance to the measures as required by its Regional Reliability Organization.

Exception Reporting: Each Region shall report compliance and violations to NERC via the NERC compliance reporting process.

1.2. Compliance Monitoring Period and Reset Time Frame

Periodic Review: Entities will be selected for operational reviews at least every three years. One calendar year without a violation from the time of the violation.

1.3. Data Retention

Not specified.

1.4. Additional Compliance Information

Not specified.

2. Violation Severity Levels:

R#	Lower	Moderate	High	Severe
R1	N/A	N/A	N/A	The ISN data recipient failed to sign the NERC Confidentiality Agreement for “Electric System Reliability Data”.
R2	The responsible entity failed to provide any of the data requested by other Balancing Authorities or Transmission Operators.	N/A	N/A	The responsible entity failed to provide all of the data requested by its host Balancing Authority or Transmission Operator.
R3	The responsible entity failed to provide any of the data requested by other Balancing Authorities or Transmission Operators.	N/A	N/A	The responsible entity failed to provide all of the data requested by its host Balancing Authority or Transmission Operator.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1		Removed the Reliability Coordinator from the list of responsible functional entities Deleted R1 and R1.1 Modified M1 to omit the reference to the Reliability Coordinator Deleted VSLs for R1 and R1.1	Revised
2	October 17, 2008	Adopted by NERC Board of Trustees	New
2	March 23, 2011	Order issued by FERC approving TOP-005-2 (approval effective 5/23/11)	
2a	April 21, 2011	Added FERC approved Interpretation	

Attachment 1-TOP-005

Electric System Reliability Data

This Attachment lists the types of data that Balancing Authorities, and Transmission Operators are expected to share with other Balancing Authorities and Transmission Operators.

1. The following information shall be updated at least every ten minutes:

1.1. Transmission data. Transmission data for all Interconnections plus all other facilities considered key, from a reliability standpoint:

1.1.1 Status.

1.1.2 MW or ampere loadings.

1.1.3 MVA capability.

1.1.4 Transformer tap and phase angle settings.

1.1.5 Key voltages.

1.2. Generator data.

1.2.1 Status.

1.2.2 MW and MVAR capability.

1.2.3 MW and MVAR net output.

1.2.4 Status of automatic voltage control facilities.

1.3. Operating reserve.

1.3.1 MW reserve available within ten minutes.

1.4. Balancing Authority demand.

1.4.1 Instantaneous.

1.5. Interchange.

1.5.1 Instantaneous actual interchange with each Balancing Authority.

1.5.2 Current Interchange Schedules with each Balancing Authority by individual Interchange Transaction, including Interchange identifiers, and reserve responsibilities.

1.5.3 Interchange Schedules for the next 24 hours.

1.6. Area Control Error and frequency.

1.6.1 Instantaneous area control error.

1.6.2 Clock hour area control error.

1.6.3 System frequency at one or more locations in the Balancing Authority.

2. Other operating information updated as soon as available.

2.1. Interconnection Reliability Operating Limits and System Operating Limits in effect.

2.2. Forecast of operating reserve at peak, and time of peak for current day and next day.

2.3. Forecast peak demand for current day and next day.

2.4. Forecast changes in equipment status.

2.5. New facilities in place.

2.6. New or degraded special protection systems.

2.7. Emergency operating procedures in effect.

2.8. Severe weather, fire, or earthquake.

2.9. Multi-site sabotage.

Appendix 2

Requirement Number and Text of Requirement
TOP-005-1 Requirement R3[1] Upon request, each Balancing Authority and Transmission Operator shall provide to other Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability, the operating data that are necessary to allow these Balancing Authorities and Transmission Operators to perform operational reliability assessments and to coordinate reliable operations. Balancing Authorities and Transmission Operators shall provide the types of data as listed in Attachment 1-TOP-005-0 "Electric System Reliability Data," unless otherwise agreed to by the Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability. *The above-referenced Attachment 1 — TOP-005-0 specifies the following data as item 2.6:* New or degraded special protection systems. *[Underline added for emphasis.]* **IRO-005-1 Requirement R12** **R12.** Whenever a Special Protection System that may have an inter-Balancing Authority, or inter-Transmission Operator impact (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation) is armed, the Reliability Coordinators shall be aware of the impact of the operation of that Special Protection System on inter-area flows. The Transmission Operator shall immediately inform the Reliability Coordinator of the status of the Special Protection System including any degradation or potential failure to operate as expected. *[Underline added for emphasis.]* **PRC-012-0 Requirements R1 and R1.3** **R1.** Each Regional Reliability Organization with a Transmission Owner, Generator Owner, or Distribution Providers that uses or is planning to use an SPS shall have a documented Regional Reliability Organization SPS review procedure to ensure that SPSs comply with Regional criteria and NERC Reliability Standards. The Regional SPS review procedure shall include: **R1.3.** Requirements to demonstrate that the SPS shall be designed so that a single SPS component failure, when the SPS was intended to operate, does not prevent the interconnected transmission system from meeting the performance requirements defined in Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.
Background Information for Interpretation
The TOP-005-1 standard focuses on two key obligations. The first key obligation (Requirement R1) is a "responsibility mandate." Requirement R1 establishes who is responsible for the obligation to provide operating data "required" by a Reliability Coordinator within the framework of the Reliability Coordinator requirements defined in the IRO standards. The second key obligation (Requirement R3) is a "performance mandate." Requirement R3 defines the obligation to provide data "requested" by other reliability entities that is needed "to perform assessments and to coordinate operations." The Attachment to TOP-005-1 is provided as a guideline of what "can be shared." The Attachment is not an obligation of "what must be shared." Enforceable NERC Requirements must be explicitly contained within a given Standard's approved requirements. In this case, the standard only requires data "upon request." If a Reliability Coordinator or other reliability entity were to request data such as listed in the

[1] In the current version of the Standard (TOP-005-2a), this requirement is R2.

Attachment, then the entity being asked would be mandated by Requirements R1 and R3 to provide that data (including item 2.6, whether it is or is not in some undefined "degraded" state).

IRO-002-1 requires the Reliability Coordinator to have processes in place to support its reliability obligations (Requirement R2). Requirement R4 mandates that the Reliability Coordinator have communications processes in place to meet its reliability obligations, and Requirement R5 et al mandate the Reliability Coordinator to have the tools to carry out these reliability obligations.

IRO-003-2 (Requirements R1 and R2) requires the Reliability Coordinator to monitor the state of its system.

IRO-004-1 requires that the Reliability Coordinator carry out studies to identify Interconnection Reliability Operating Limits (Requirement R1) and to be aware of system conditions via monitoring tools and information exchange.

IRO-005-1 mandates that each Reliability Coordinator monitor predefined base conditions (Requirement R1), collect additional data when operating limits are or may be exceeded (Requirement R3), and identify actual or potential threats (Requirement R5). The basis for that request is left to each Reliability Coordinator. The Purpose statement of IRO-005-1 focuses on the Reliability Coordinator's obligation to be aware of conditions that may have a "significant" impact upon its area and to communicate that information to others (Requirements R7 and R9). Please note: it is from this communication that Transmission Operators and Balancing Authorities would either obtain or would know to ask for SPS information from another Transmission Operator.

The IRO-005-1 (Requirement R12) standard implies that degraded is a condition that will result in a failure to operate as designed. If the loss of a communication channel will result in the failure of an SPS to operate as designed then the Transmission Operator would be mandated to report that information. On the other hand, if the loss of a communication channel will not result in the failure of the SPS to operate as designed, then such a condition can be, but is not mandated to be, reported.

Conclusion

The TOP-005-1 standard does not provide, nor does it require, a definition for the term "degraded."

The IRO-005-1 (R12) standard implies that degraded is a condition that will result in a failure of an SPS to operate as designed. If the loss of a communication channel will result in the failure of an SPS to operate as designed, then the Transmission Operator would be mandated to report that information. On the other hand, if the loss of a communication channel will not result in the failure of the SPS to operate as designed, then such a condition can be, but is not mandated to be, reported.

To request a formal definition of the term degraded, the Reliability Standards Development Procedure requires the submittal of a Standards Authorization Request.

A. Introduction

1. Title: **Automatic Voltage Regulators (AVR)**

2. Number: VAR-002-WECC-1

3. Purpose: To ensure that Automatic Voltage Regulators on synchronous generators and condensers shall be kept in service and controlling voltage.

4. Applicability

4.1. Generator Operators

4.2. Transmission Operators that operate synchronous condensers

4.3. This VAR-002-WECC-1 Standard only applies to synchronous generators and synchronous condensers that are connected to the Bulk Electric System.

5. Effective Date: On the first day of the first quarter, after applicable regulatory approval.

B. Requirements

R1. Generator Operators and Transmission Operators shall have AVR in service and in automatic voltage control mode 98% of all operating hours for synchronous generators or synchronous condensers. Generator Operators and Transmission Operators may exclude hours for R1.1 through R1.10 to achieve the 98% requirement. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

R1.1. The synchronous generator or synchronous condenser operates for less than five percent of all hours during any calendar quarter.

R1.2. Performing maintenance and testing up to a maximum of seven calendar days per calendar quarter.

R1.3. AVR exhibits instability due to abnormal system configuration.

R1.4. Due to component failure, the AVR may be out of service up to 60 consecutive days for repair per incident.

R1.5. Due to a component failure, the AVR may be out of service up to one year provided the Generator Operator or Transmission Operator submits documentation identifying the need for time to obtain replacement parts and if required to schedule an outage.

R1.6. Due to a component failure, the AVR may be out of service up to 24 months provided the Generator Operator or Transmission Operator submits documentation identifying the need for time for excitation system replacement (replace the AVR, limiters, and controls but not necessarily the power source and power bridge) and to schedule an outage.

R1.7. The synchronous generator or synchronous condenser has not achieved Commercial Operation.

R1.8. The Transmission Operator directs the Generator Operator to operate the synchronous generator, and the AVR is unavailable for service.

R1.9. The Reliability Coordinator directs Transmission Operator to operate the synchronous condenser, and the AVR is unavailable for service.

R1.10. If AVR exhibits instability due to operation of a Load Tap Changer (LTC) transformer in the area, the Transmission Operator may authorize the Generator Operator to operate the excitation system in modes other than automatic voltage control until the system configuration changes.

R2. Generator Operators and Transmission Operators shall have documentation identifying

the number of hours excluded for each requirement in R1.1 through R1.10. *[Violation Risk Factor: Low] [Time Horizon: Operations Assessment]*

C. Measures

M1. Generator Operators and Transmission Operators shall provide quarterly reports to the compliance monitor and have evidence for each synchronous generator and synchronous condenser of the following:

M1.1 The actual number of hours the synchronous generator or synchronous condenser was on line.

M1.2 The actual number of hours the AVR was out of service.

M1.3 The AVR in service percentage.

M1.4 If excluding AVR out of service hours as allowed in R1.1 through R1.10, provide:

M1.4.1 The number of hours excluded, and

M1.4.2 The adjusted AVR in-service percentage.

M2. If excluding hours for R1.1 through R1.10, provide the date of the outage, the number of hours out of service, and supporting documentation for each requirement that applies.

D. Compliance

1. Compliance Monitoring Process

1.1 Compliance Monitoring Responsibility

Compliance Enforcement Authority

1.2 Compliance Monitoring Period

Compliance Enforcement Authority may use one or more of the following methods to assess compliance:

- Reports submitted quarterly
- Spot check audits conducted anytime with 30 days notice
- Periodic audit as scheduled by the Compliance Enforcement Authority
- Investigations
- Other methods as provided for in the Compliance Monitoring Enforcement Program

The Reset Time Frame shall be a calendar quarter.

1.3 Data Retention

The Generator Operators and Transmission Operators shall keep evidence for Measures M1 and M2 for three years plus current year, or since the last audit, whichever is longer.

1.4 Additional Compliance Information

1.4.1 The sanctions shall be assessed on a calendar quarter basis.

1.4.2 If any of R1.2 through R1.9 continues from one quarter to another, the number of days accumulated will be the contiguous calendar days from the beginning of the incident to the end of the incident. For example, in R1.4 if the 60 day repair period goes beyond the end of a quarter, the repair period does not reset at the beginning of the next quarter.

1.4.3 When calculating the in-service percentages, do not include the time the AVR is out of service due to R1.1 through R1.10.

1.4.4 The standard shall be applied on a machine-by-machine basis (a Generator Operator or Transmission Operator can be subject to a separate sanction for each non-compliant synchronous generator and synchronous condenser).

2. Violation Severity Levels for R1

2.1. Lower: There shall be a Lower Level of non-compliance if the following condition exists:

2.1.1. AVR is in service less than 98% but at least 90% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.

2.2. Moderate: There shall be a Moderate Level of non-compliance if the following condition exists:

2.2.1. AVR is in service less than 90% but at least 80% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.

2.3. High: There shall be a High Level of non-compliance if the following condition exists:

2.3.1. AVR is in service less than 80% but at least 70% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.

2.4. Severe: There shall be a Severe Level of non-compliance if the following condition exists:

2.4.1. AVR is in service less than 70% of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.

3. Violation Severity Levels for R2

3.1. Lower: There shall be a Lower Level of non-compliance if documentation is incomplete with any requirement R1.1 through R1.10.

3.2. Moderate: There shall be a Moderate Level of non-compliance if the Generator Operator does not have documentation to demonstrate compliance with any requirement R1.1 through R1.10.

3.3. High: Not Applicable

3.4. Severe: Not Applicable

E. Regional Differences

Version History — Shows Approval History and Summary of Changes in the Action Field

Version	Date	Action	Change Tracking
1	April 16, 2008	Permanent Replacement Standard for VAR-STD-002a-1	
1	April 21, 2011	FERC Order issued approving VAR-002-WECC-1 (approval effective June 27, 2011)	

A. Introduction

1. **Title:** **Power System Stabilizer (PSS)**
2. **Number:** VAR-501-WECC-1
3. **Purpose:** To ensure that Power System Stabilizers (PSS) on synchronous generators shall be kept in service.
4. **Applicability**

   4.1. Generator Operators
5. **Effective Date:** On the first day of the first quarter, after applicable regulatory approval.

B. Requirements

R1. Generator Operators shall have PSS in service 98% of all operating hours for synchronous generators equipped with PSS. Generator Operators may exclude hours for R1.1 through R1.12 to achieve the 98% requirement. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

R1.1. The synchronous generator operates for less than five percent of all hours during any calendar quarter.

R1.2. Performing maintenance and testing up to a maximum of seven calendar days per calendar quarter.

R1.3. PSS exhibits instability due to abnormal system configuration.

R1.4. Unit is operating in the synchronous condenser mode (very near zero real power level).

R1.5. Unit is generating less power than its design limit for effective PSS operation.

R1.6. Unit is passing through a range of output that is a known "rough zone" (range in which a hydro unit is experiencing excessive vibration).

R1.7. The generator AVR is not in service.

R1.8. Due to component failure, the PSS may be out of service up to 60 consecutive days for repair per incident.

R1.9. Due to a component failure, the PSS may be out of service up to one year provided the Generator Operator submits documentation identifying the need for time to obtain replacement parts and if required to schedule an outage.

R1.10. Due to a component failure, the PSS may be out of service up to 24 months provided the Generator Operator submits documentation identifying the need for time for PSS replacement and to schedule an outage.

R1.11. The synchronous generator has not achieved Commercial Operation.

R1.12. The Transmission Operator directs the Generator Operator to operate the synchronous generator, and the PSS is unavailable for service.

R2. Generator Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.12. *[Violation Risk Factor: Low] [Time Horizon: Operations Assessment]*

C. Measures

M1. Generators Operators shall provide quarterly reports to the compliance monitor and have evidence for each synchronous generator of the following:

M1.1 The number of hours the synchronous generator was on line.

M1.2 The number of hours the PSS was out of service with generator on line.

M1.3 The PSS in service percentage

M1.4 If excluding PSS out of service hours as allowed in R1.1 through R1.12, provide:

M1.4.1 The number of hours excluded, and

M1.4.2 The adjusted PSS in-service percentage.

M2. If excluding hours for R1.1 through R1.12, provide:

M2.1 The date of the outage

M2.2 Supporting documentation for each requirement that applies

D. Compliance

1. Compliance Monitoring Process

1.1 Compliance Monitoring Responsibility

Compliance Enforcement Authority

1.2 Compliance Monitoring Period

Compliance Enforcement Authority may use one or more of the following methods to assess compliance:

- Reports submitted quarterly
- Spot check audits conducted anytime with 30 days notice
- Periodic audit as scheduled by the Compliance Enforcement Authority
- Investigations
- Other methods as provided for in the Compliance Monitoring Enforcement Program

The Reset Time Frame shall be a calendar quarter.

1.3 Data Retention

The Generator Operators shall keep evidence for Measures M1 and M2 for three years plus current year, or since the last audit, whichever is longer.

1.4 Additional Compliance Information

1.4.1 The sanctions shall be assessed on a calendar quarter basis.

1.4.2 If any of R1.2 through R1.12 continues from one quarter to another, the number of days accumulated will be the contiguous calendar days from the beginning of the incident to the end of the incident. For example, in R1.8 if the 60 day repair period goes beyond the end of a quarter, the repair period does not reset at the beginning of the next quarter.

1.4.3 When calculating the adjusted in-service percentage, the PSS out of service hours do not include the time associated with R1.1 through R1.12.

1.4.4 The standard shall be applied on a generating unit by generating unit basis (a Generator Operator can be subject to a separate sanction for each non-compliant synchronous generating unit or to a single sanction for multiple machines that operate as one unit).

2. Violation Severity Levels

2.1. Lower: There shall be a Lower Level of non-compliance if the following condition exists:

2.1.1. PSS is in service less than 98% but at least 90% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.

2.2. Moderate: There shall be a Moderate Level of non-compliance if the following condition exists:

2.2.1. PSS is in service less than 90% but at least 80% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.

2.3. High: There shall be a High Level of non-compliance if the following condition exists:

2.3.1. PSS is in service less than 80% but at least 70% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.

2.4. Severe: There shall be a Severe Level of non-compliance if the following condition exists:

2.4.1. PSS is in service less than 70% of all hours during which the synchronous generating unit is on line for each calendar quarter.

3. Violation Severity Levels for R2

3.1. Lower: There shall be a Lower Level of non-compliance if documentation is incomplete with any requirement R1.1 through R1.12.

3.2. Moderate: There shall be a Moderate Level of non-compliance if the Generator Operator does not have documentation to demonstrate compliance with any requirement R1.1 through R1.12.

3.3. High: Not Applicable

3.4. Severe: Not Applicable

E. Regional Differences

Version History — Shows Approval History and Summary of Changes in the Action Field

Version	Date	Action	Change Tracking
1	April 16, 2008	Permanent Replacement Standard for VAR-STD-002b-1	
1	April 21, 2011	FERC Order issued approving VAR-501-WECC-1 (approval effective June 27, 2011)	

Standard	Requirement Name	Requirement Text
BAL-005-0.1b	R2.	Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.
CIP-001-2a	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.
CIP-003-3	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-3	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
CIP-003-3	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
CIP-003-3	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
CIP-003-3	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
CIP-003-3	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-4	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
CIP-003-4	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
CIP-003-4	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Standard	Requirement Name	Requirement Text
CIP-005-3a	R2.6.	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
CIP-005-4a	R2.6.	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
CIP-007-3	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
COM-001-1.1	R6.	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001, “NERCNet Security Policy.”
EOP-004-1	R1.	Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.
EOP-005-2	R3.1.	If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.
EOP-009-0	R2.	The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.
FAC-002-1	R2.	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).
FAC-008-1	R1.3.5.	Other assumptions.
FAC-008-1	R2.	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

Standard	Requirement Name	Requirement Text
FAC-008-1	R3.	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.
FAC-008-3	R4.	Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.
FAC-008-3	R5.	If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.
FAC-013-2	R3.	If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.
INT-007-1	R1.2.	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.
IRO-016-1	R2.	The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.
MOD-004-1	R1.	The Transmission Service Provider that maintains CBM shall prepare and keep current a "Capacity Benefit Margin Implementation Document" (CBMID) that includes, at a minimum, the following information:

Standard	Requirement Name	Requirement Text
MOD-004-1	R1.1.	The process through which a Load-Serving Entity within a Balancing Authority Area associated with the Transmission Service Provider, or the Resource Planner associated with that Balancing Authority Area, may ensure that its need for Transmission capacity to be set aside as CBM will be reviewed and accommodated by the Transmission Service Provider to the extent Transmission capacity is available.
MOD-004-1	R1.2.	The procedure and assumptions for establishing CBM for each Available Transfer Capability (ATC) Path or Flowgate.
MOD-004-1	R1.3.	The procedure for a Load-Serving Entity or Balancing Authority to use Transmission capacity set aside as CBM, including the manner in which the Transmission Service Provider will manage situations where the requested use of CBM exceeds the amount of CBM available.
MOD-004-1	R10.	The Load-Serving Entity or Balancing Authority shall request to import energy over firm Transfer Capability set aside as CBM only when experiencing a declared NERC Energy Emergency Alert (EEA) 2 or higher.
MOD-004-1	R11.	When reviewing an Arranged Interchange using CBM, all Balancing Authorities and Transmission Service Providers shall waive, within the bounds of reliable operation, any Real-time timing and ramping requirements.
MOD-004-1	R12.	The Transmission Service Provider that maintains CBM shall approve, within the bounds of reliable operation, any Arranged Interchange using CBM that is submitted by an “energy deficient entity” under an EEA 2 if:
MOD-004-1	R12.1.	The CBM is available
MOD-004-1	R12.2.	The EEA 2 is declared within the Balancing Authority Area of the “energy deficient entity,” and
MOD-004-1	R12.3.	The Load of the “energy deficient entity” is located within the Transmission Service Provider’s area.
MOD-004-1	R2.	The Transmission Service Provider that maintains CBM shall make available its current CBMID to the Transmission Operators, Transmission Service Providers, Reliability Coordinators, Transmission Planners, Resource Planners, and Planning Coordinators that are within or adjacent to the Transmission Service Provider’s area, and to the Load Serving Entities and Balancing Authorities within the Transmission Service Provider’s area, and notify those entities of any changes to the CBMID prior to the effective date of the change.
MOD-004-1	R3.	Each Load-Serving Entity determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by:

Standard	Requirement Name	Requirement Text
MOD-004-1	R3.1.	Using one or more of the following to determine the GCIR: Loss of Load Expectation (LOLE) studies; Loss of Load Probability (LOLP) studies; Deterministic risk-analysis studies; Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R3.2.	Identifying expected import path(s) or source region(s).
MOD-004-1	R4.	Each Resource Planner determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by:
MOD-004-1	R4.1.	Using one or more of the following to determine the GCIR: Loss of Load Expectation (LOLE) studies; Loss of Load Probability (LOLP) studies; Deterministic risk-analysis studies; Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R4.2.	Identifying expected import path(s) or source region(s).
MOD-004-1	R5.	At least every 13 months, the Transmission Service Provider that maintains CBM shall establish a CBM value for each ATC Path or Flowgate to be used for ATC or Available Flowgate Capability (AFC) calculations during the 13 full calendar months (months 2-14) following the current month (the month in which the Transmission Service Provider is establishing the CBM values). This value shall:
MOD-004-1	R5.1.	Reflect consideration of each of the following if available: Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Service Provider's area; Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Service Provider’s area; Any reserve margin or resource adequacy requirements for loads within the Transmission Service Provider’s area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R5.2.	Be allocated as follows: For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners; For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Service Provider

Standard	Requirement Name	Requirement Text
MOD-004-1	R6.	At least every 13 months, the Transmission Planner shall establish a CBM value for each ATC Path or Flowgate to be used in planning during each of the full calendar years two through ten following the current year (the year in which the Transmission Planner is establishing the CBM values). This value shall:
MOD-004-1	R6.1.	Reflect consideration of each of the following if available: Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Planner's area; Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Planner's area; Any reserve margin or resource adequacy requirements for loads within the Transmission Planner's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R6.2.	Be allocated as follows: For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners; For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Planner.
MOD-004-1	R7.	Less than 31 calendar days after the establishment of CBM, the Transmission Service Provider that maintains CBM shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the Transmission Service Provider's system of the amount of CBM set aside.
MOD-004-1	R8.	Less than 31 calendar days after the establishment of CBM, the Transmission Planner shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the system being planned by the Transmission Planner of the amount of CBM set aside.
MOD-004-1	R9.	The Transmission Service Provider that maintains CBM and the Transmission Planner shall each provide (subject to confidentiality and security requirements) copies of the applicable supporting data, including any models, used for determining CBM or allocating CBM over each ATC Path or Flowgate to the following:
MOD-004-1	R9.1.	Each of its associated Transmission Operators within 30 calendar days of their making a request for the data.
MOD-004-1	R9.2.	To any Transmission Service Provider, Reliability Coordinator, Transmission Planner, Resource Planner, or Planning Coordinator within 30 calendar days of their making a request for the data.
NUC-001-2	R9.1.	Administrative elements:

Standard	Requirement Name	Requirement Text
NUC-001-2	R9.1.1.	Definitions of key terms used in the agreement.
NUC-001-2	R9.1.2.	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.
NUC-001-2	R9.1.3.	A requirement to review the agreement(s) at least every three years.
NUC-001-2	R9.1.4.	A dispute resolution mechanism.
PRC-008-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.
PRC-008-0	R2.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).
PRC-009-0	R1.	The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:
PRC-009-0	R1.1.	A description of the event including initiating conditions.
PRC-009-0	R1.2.	A review of the UFLS set points and tripping times.
PRC-009-0	R1.3.	A simulation of the event.
PRC-009-0	R1.4.	A summary of the findings.
PRC-009-0	R2.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.
PRC-010-0	R2.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

Standard	Requirement Name	Requirement Text
PRC-022-1	R2.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.
TOP-001-1a	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.
TOP-005-2a	R1.	As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for “Electric System Reliability Data.”
VAR-002-WECC-1	R2.	Generator Operators and Transmission Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.10.
VAR-501-WECC-1	R2.	Generator Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.12.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2013-02 Retirement of Reliability Standard Requirements

Unofficial Comment Form for Paragraph 81 (P81) Project —Retirement of Reliability Standard Requirements

This form is provided in a Word format for the development of your internal drafts only.

Please use the electronic comment form located at the link below to submit official comments on the P81 Project. Comments must be submitted by **September 4, 2012.** If you have questions, please contact Kristin Iwanechko at Kristin.Iwanechko@nerc.net or by telephone at 404-446-9736.

http://www.nerc.com/filez/standards/Project2013-02_Paragraph_81.html

Background Information:
On September 30, 2011, the North American Electric Reliability Corporation (NERC) filed a petition with the Federal Energy Regulatory Commission (FERC) requesting approval of its proposal to make informational filings in a "Find, Fix, Track and Report" (FFT) spreadsheet of lesser-risk, remediated possible violations of Reliability Standards. On March 15, 2012, the FERC issued an order conditionally accepting NERC's FFT proposal. In paragraph 81 (P81) of that order, the FERC also that stated:

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved

> Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, a draft Standards Authorization Request (SAR) was drafted to set forth criteria and a process to identify Reliability Standard requirements that either: (a) provide little protection to the Bulk Electric System; (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file the identified Reliability Standard requirements with FERC to have them removed from the FERC-approved list of Reliability Standards.

Standards Process Input Group (SPIG)

In addition to addressing P81, the draft SAR was drafted consistent with what the SPIG developed as Recommendation No. 4, as set forth in *NERC's Recommendations to Improve The Standards Development Process* on page *12* (April 2012), which states:

Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

Collaborative Process

The draft SAR and the suggested list of Reliability Standard requirements embedded in the SAR for consideration in the Initial Phase are the product of collaborative discussions among the following entities and their members: Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group.

It is hoped the time, effort and resources dedicated to the collaborative discussions have resulted in a reasonable SAR and an appropriately-scoped list of Reliability Standard requirements for the Initial Phase. It is also noted the statements accompanying each of the identified Reliability Standard requirements are the beginning of, and not necessarily a complete technical justification for, retirement of the requirements. It is also understood that the P81 Standards Drafting Team will need to coordinate discussions with other active Standard Drafting Teams concerning the retirement of certain Reliability Standard requirements.

To obtain input on the draft SAR, the P81 Standards Drafting Team is posting the draft SAR for stakeholder comment for a 30-day comment period. Accordingly, it is requested that you submit your comments by **September 4, 2012** via the electronic comment form.

Questions

1. **Do you agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement?**

   If not, please explain in the comment area.

   ☐ Yes

   ☐ No

   Comments:

2. **The Initial Phase of the P81 project is designed to identify all FERC-approved Reliability Standard requirements that easily satisfy the criteria. Do you agree that the suggested list of Reliability Standard requirements included in the draft SAR easily satisfy the criteria listed in the draft SAR? If you disagree, please provide a statement supporting what Reliability Standard requirements you would add or subtract from the Initial Phase, including a citation to at least one element of Criterion B, as applicable.**

   ☐ Yes

   ☐ No

   Comments:

3. **The subsequent phases of the P81 project are designed to identify all FERC-approved Reliability Standard requirements that could not be included in the Initial Phase due to the need for additional analysis or an editing of language. Please list any Reliability Standard requirements that you believe should be revised or retired in a subsequent phase, and include a brief supporting statement and citation to at least one element of Criterion B for each requirement listed.**

   Comments:

4. **If you have any other comments or suggestions on the draft SAR that you have not already provided in response to the previous questions, please provide them here.**

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-02 Paragraph 81

Informal Comment Period Now Open: August 3 – September 4, 2012

Now Available

The Standards Committee has authorized posting of this draft Standards Authorization Request (SAR) for stakeholder input for 30 days.

Instructions

An informal comment period is open through 8 p.m. Eastern on **Monday, September 4, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

A webinar on the draft SAR will be conducted on August 21, 2012 from 2-3 p.m. Eastern and will be announced in a separate email with the registration link.

The drafting team will review the comments and determine whether to revise the SAR before proceeding with Phase 1 of the project. The drafting team will post a summary of its responses to comments received during this informal comment period.

Background

On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated the following in Paragraph 81:

> "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when

these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES," are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs. The draft SAR identifies criteria for retiring or modifying requirements, defines phases for the project, and includes a suggested list of requirements put together by NERC, the regions, and the trades and their member companies for consideration in Phase 1. The suggested list includes requirements in 28 Reliability Standards. Phase 1 identifies Reliability Standard requirements that clearly meet the criteria set forth in the SAR and are believed to not require extensive technical research. Subsequent phases of the project will address Reliability Standard requirements that need additional technical research before retirement or modification.

To sign up for the plus list for this project to follow along with meetings and work products, please email Kristin Iwanechko.

Standards Development Process

The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Name (29 Responses)
Organization (29 Responses)
Group Name (14 Responses)
Lead Contact (14 Responses)
Contact Organization (14 Responses)
Question 1 (43 Responses)
Question 1 Comments (43 Responses)
Question 2 (43 Responses)
Question 2 Comments (43 Responses)
Question 3 (0 Responses)
Question 3 Comments (43 Responses)
Question 4 (0 Responses)
Question 4 Comments (43 Responses)

Group
Northeast Power Coordinating Council
Lee Pedowicz
Northeast Power Coordinating Council
Yes
NPCC participating members support the P81 initiative and agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement. The criteria are also consistent with FERC's guidance in Paragraph 81 of the FFT Order. With respect to the words in Criterion A wording, it could be interpreted as an indication that the original reliability standard requirement was a mistake. Suggest the SDT consider alternative wording to indicate that the experience with the requirement, over time, has proven not to be useful to accomplish its initially intended reliability objective, or has not produced clear results for the initially intended reliability objective. Criterion A, and Technical Criteria B9 "Little, if any, value as a reliability requirement" are redundant.
No
From page 25 of the SAR, "Since PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 provides little protection to the BES and better handled under event analysis and lessons learned papers, it should be removed." is not valid due to that fact that as of this posting the Event Analysis Program (EAP) has not become part of the RoP and is therefore a voluntary program. The requirements that are covered by these standards are mandatory cannot be replaced by a voluntary program. Refer to the following: Additionally, the EAP process is an after-the-fact Analysis of an event or events. These standard requirements (PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2) address different needs which can be determined only if such an event occurs. For example, from PRC-008-0--"R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance." This requirement addresses the need to have an equipment maintenance and testing program in place prior to an event. Discovering that an entity did not have this as a result of an event analysis would, in this case, be after the damage is done and would not serve reliability. Analyzing why the UFSL program did not operate properly would come under the purview of the EAP but that is different from the Standard's intent. PRC-008-0--"R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days)." If the EAP was relied upon to meet this requirement the receipt or confirmation of this program would only occur after an event. PRC-009-0--"R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The

analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to: R1.1 A description of the event including initiating conditions. R1.2 A review of the UFLS set points and tripping times. R1.3 A simulation of the event. R1.4 A summary of the findings." Although this Standard appears that it could be covered under EAP, it is a highly detailed technical study and needs to be carried out on its own accord. Event Analysis will focus primarily what caused the event that triggered the UFLS program but not necessarily the program itself. Because of the importance of the UFLS program to the reliability of the system, its performance should not be analyzed only on a voluntary basis and not only by those entities that actually shed load as a result of the event, but against the whole regional program. PRC-009-0--“R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.” This is administrative, refer to the response for R1 preceding. PRC-010-0--“R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).” This should not triggered only after an event, see preceding response for R1 preceding. PRC-022-1--“R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.” This is the same situation as for the UFLS program. Refer to the responses preceding. IRO-014-2 --The following requirements in Standard IRO-014-2 are administrative requirements only and do not enhance reliability, and should be considered for removal in the Initial Phase. “R2. Each Reliability Coordinator shall maintain its Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 as follows: [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning] 2.1. Review and update annually with no more that 15 months between reviews. 2.2. Obtain written agreement from all of the Reliability Coordinators required to take the indicated action(s) for each update. 2.3. Distribute to all Reliability Coordinators that are required to take the indicated action(s) within 30 days of an update.” FAC-003-1 Requirements R3, and R4 (shown below) and their sub-requirements are administrative (reporting) requirements only and do not enhance reliability, and should be considered for removal in the Initial Phase. R3. The Transmission Owner shall report quarterly to its RRO, or the RRO’s designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation. R4. The RRO shall report the outage information provided to it by Transmission Owner’s, as required by Requirement 3, quarterly to NERC, as well as any actions taken by the RRO as a result of any of the reported outages. In addition, as shown below, CIP-005-3 R4 and CIP-007-3 R8 are essentially the same. Suggest to eliminate CIP-005-3 R4 and include assessment of access points in CIP-007-3 R8. CIP-005-3 R4: "R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following: R4.1. A document identifying the vulnerability assessment process; R4.2. A review to verify that only ports and services required for operations at these access points are enabled; R4.3. The discovery of all access points to the Electronic Security Perimeter; R4.4. A review of controls for default accounts, passwords, and network management community strings; R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan." CIP-007-3 R8: "R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following: R8.1 A document identifying the vulnerability assessment process; R8.2 A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled; R8.3 A review of controls for default accounts; and, R8.4 Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan."
Individual

Nazra Gladu
Manitoba Hydro
Yes
The technical criteria B.9, "Little if any, value as a reliability requirement", is very subjective and should be redefined or clarified.
Yes
The following statement should be removed from the standard as it does not support reliability of the BES [B8]: FAC-013-2 R5. 'However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request' The following statement should be removed from the standard as it does not support reliability or provide any protection to the BES. [B8]: FAC-013-2 R6. 'If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information'.
It is not clear what will happen in instances where this project proposes to remove a requirement from a FERC approved Reliability Standard when the NERC BOT has already approved a newer version of that same standard. Will the newer BOT approved version also be modified if it includes one of the requirements in question? What if industry has already resolved one of these issues in the next version of a standard? Shouldn't we just implement the newer version?
Individual
Scott McGough
Georgia System Operations Corporation
Yes
Georgia System Operations agrees with the criteria listed in the SAR to identify Reliability Standard requirements for either modification or withdrawal.
Yes
Georgia System Operations agrees with the suggested list of Reliability Standard requirements contained in the SAR for the Initial Phase of P81.
EOP-002-3, R1 PER-001-0.1, R1 Criteria B7, 9 Statement: reference to BA or RC responsibilities and authority are within the criteria of NERC's Functional Model and so this is redundant. In addition, it is understood that these functions are substantial if not paramount for an entity to become certified as such. FAC-001-0 (all requirements) Criteria B 1, 3 and 6 Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. All INT standards Criteria B 1, 3 and 6 Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Reliability Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Note: INT-007-1 R1.2 is part of Initial Phase. All data collection requirements CIP-005-3a, 4a R5.3 CIP-006c, -4c R7, R8.3 CIP-007-3, -4 R5.1.2; R6.4; R7.3 CIP-008-3, -4 R2 PRC-018-1, R5 Criteria B1,2 and 9 Statement: These requirements are for data retention and although the need is substancial, i.e. as a sort of forensic tool, they serve no function to reliability from an immediate time perspective. Standards currently requiring reporting. Criteria 1, 4 and 9 EOP-002-3 R9.2 EOP-004-1 R3 and its subrequirements; R4 and R5 FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4 FAC-010-2.1 R5 FAC-011-2 R5 FAC-013-2 R6 MOD-012-0 R2 MOD-020-0 R1 MOD-021-1 R3 PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3. PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2 TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2. Statement: These are all reporting requirements; they do not aid reliability from an immediate time perspective. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the

Reliability Standards. Requirements applied to annual reviews Criteria B1, 2,3 7 and 9 CIP-002-2, -4 R4 CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3 CIP-006-3c, -4 R1.8 CIP-007-3, -4 R9 CIP-009-3, -4 R1 EOP-005-1 R1; EOP-005-2 R3.1 EOP-008-0 R1.7 EOP-008-1 R5 IRO-014-1 R4.3 Statement: These requirements do not closely relate to operations of the Bulk Electric System. They would be better served as processes expected of entities to manage their compliance programs and processes. PRC-005-1b, R2 Criteria B4, 9 Statement: This requirement needs to be revised such that language is elminated as it refers to the entity providing to its RE within 30 days. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9 Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard.
Reliability Standard requirements are those that provide for Reliable Operation, including without limiting the foregoing, requirements for the operation of existing Facilities, including cyber security protection, and including the design of planned additions or modifications to such Facilities to the extent necessary for Reliable Operation. NERC administers other programs, such as industry alerts, reliability assessments, event and trend analyses, education, and monitoring and enforcing Reliability Standards. These other programs are designed to work in concert with Reliability Standards to support reliable operation. NERC requirements relating to administering these other programs are very important but are not Reliability Standard requirements. One of the criteria for evaluating the elimination of a Reliability Standard requirement is that it is purely reporting. There are a number of NERC requirements for these other NERC programs embedded in Reliability Standards. Most of them are purely reporting. However, to the extent that there may be other requirements for these NERC programs embedded that are not purely reporting, they should also be considered for elimination. Reliability Standards by definition are not mechanisms for the administration of those other NERC programs.
Individual
Ronnie C. Hoeinghaus
City of Garland
Yes
Yes
This is a good start on removing requirements that are either redundant or provide little / no protection for Bulk-Power System reliability.
Individual
Dan Miller
Entergy Services, Inc.
Yes
Yes
CIP-006 R5 - A revision to the language in CIP-006 R5 is needed in order to require the review and handling of incidents of unauthorized access (when a door, gate or window has been opened without authorization), as opposed to what is more accurately characterized as "unsuccessful" access attempts (e.g. invalid access card swipes). There currently is no definition of "unauthorized access attempts". The methods to be used for monitoring that are listed in the requirement, however do list: "Alarm Systems that alarm to indicate a door, gate or window has been opened without authorization". This method does not indicate that the alarm system must alarm on card swipes that do not result in the door opening, and be characterized as "Unauthorized Access attempts". Unsuccessful card swipes at a PSP access point, for example, do not suggest an unauthorized access attempt. A card swipe can be unsuccessful for a number of reasons, all of which are recorded by the key card system, such as the use of a deactivated card, an invalid card format, and a card not in the

card file. An unsuccessful card swipe itself is not an indication that a PSP access point was “opened within authorization” because it does not indicate that the door has been opened in any manner. However, in the FAQ guidance for the CIP Reliability Standards, NERC acknowledged that Responsible Entities can consider single failed access attempts such as a single failed log-in not to be suspicious events requiring a response A single failed card swipe should be treated in the same way. The rewording of this requirement would address Criteria B-8 - "Hinders the protection or reliable operation of the BES." Investigating and documenting each unsuccessful card swipe would take a tremendous amount of time and produce a significant amount of paperwork without providing any additional physical security. CIP-005 R3 and CIP-006 R5 - Revisions to the wording around the timing of monitoring both physical and electronic access are needed. CIP-005 R3 - Monitoring Electronic Access states that "The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week." and CIP-006 R5 -Monitoring Physical Access stats that "The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. The "twenty-four hours a day, seven days a week" portion of these requirements provides an unachievable requirement for 100% uptime for all systems used to monitor such access. The requirement should allow for a resonable amount of downtime. Either the "twenty-four hours a day, seven days a week" wording in these requirements could be removed altogether, or alternative langauge, such as requiring "High Availability" (for example 99.9% uptime) or some other wording that allowed for very small amounts of downtime that might be required for system reboots or minor maintenance.

For future phases, indutry input should be gathered in a more formal process to allow for suggestions for re-wording or suggesting additional requirements for removal.

Individual

Michael Falvo

Independent Electricity System Operator

No

(1) The IESO supports this proposed effort and agrees with most of the criteria, with some exceptions (except #5): “The Reliability Standard requirement requires responsible entities to periodically update (e.g., annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.” Take for example the system restoration plan. An annual review is necessary to ensure that the plan recognizes BES facility changes that occurred since the last review/update. Another example is the exceptions to the cyber security policy that needs to be reviewed and approved by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Applying this criterion in a broad brush manner without looking at each requirement may result in removing requirements that are still needed for reliability. (2) Generally, the nine criteria listed in the SAR are simple and sufficient to be used to determine retirement of reliability standard requirements. It is recommended that the word “Technical” in the heading of the B section “Technical Criteria” be erased as the criteria aren’t based on technical data. Also, it is unclear and confusing as to how the section C “Additional Data and Reference Points” will be used by the drafting team to determine retirement of reliability standards even though they have satisfied Criteria A and B. Criterion B.9 can potentially be deleted as its purpose seems to be the duplication of Criterion A. (3) The SAR narrative for TOP-001-1a R3 states the requirement is redundant with IRO-001-1a R8. IRO-001-1a does not exist; we believe, it should be IRO-001-1.1 R8 instead.

No

(1) We generally agree that most of the identified standards/requirements would meet the proposed criteria. However, as indicated under Q1, we believe that the “annual review” criterion is too broad which could result in retiring some requirements that are still needed for reliability. In addition, the acid test for retirement a requirement is when the standard drafting team reviews the overall reliability impact of removing a particular requirement from a standard, and how it may affect other related standards. In brief, it is premature to pass on this judgment at the SAR stage. We urge the SAR proponent to simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired. And, in order to meet the requirements for regulatory approval, we

suggest the SDT to provide strong technical basis to justify each retirement.
(1) IRO-004-2 R1 could be retired if the wording in IRO-001-1.1 R8 was changed to cover all operating timeframes (Criterion B7). (2) We do not have any other particular standards/requirements in mind at this time. However, we will review and propose additional candidates for future phases as this project gets into the mid or end of Phase I. We believe the industry should focus on the Phase I effort at this time to gauge the regulator's and industry's reaction before marching too far down the path.
No comments.
Individual
Michelle Clements
Wolverine Power Supply Cooperative, Inc.
Yes
Yes
Wolverine agrees with the list of requirements that the trade associations are submitting. We are a member of NRECA and agree with their comments.
Individual
Thomas C. Duffy
Central Husdon Gas & Electric Corporation
Yes
Yes
We agree with the criteria as listed, however, we believe that another criterion must be added. This criterion is that the retirement of a requirement must not create a compliance gap for Entities. Several of the NERC requirements have been crafted to afford Entities a means to display compliance. Retirement of these requirements can place an Entity's compliance efforts in jeopardy. A salient example of this is identified below: Central Hudson Gas & Electric Corporation strongly disagrees with the inclusion of CIP-003-3, -4 Requirements R3, R3.1, R3.2, R3.3 as candidates for retirement. The reasons stated in the SAR in favor of inclusion are that these requirements are administrative in nature and are purely examples of a documentation process. Further it is stated in the SAR that they, "…. have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements." This last statement is precisely the reason why the aforementioned requirements were included in the standard. These requirements allow Registered Entities to, on rare occasions, take an exception to one or several of the CIP requirements (for a limited period of time) if they (1) have valid cause (major emergency, Force Majeure, etc.), (2) document the occurrence and (3) are reviewed and approved by the CIP Senior Manager. This process supports the Registered Entity's compliance effort and acknowledges the need for special protocols to address emergency circumstances. Without such a process, the only recourse for the Registered Entity is to self-report a violation which is not within its control. In other words, retirement of these requirements would force the Registered Entity to be in full compliance with ALL CIP Standards ALL the time regardless of circumstance. The concept of 'realistic expectation' was undoubtedly the reason these requirements were crafted and included in the standard. Further, with regard to the Registered Entity's decision to claim an exception, a system of checks and balances already exists. At the time of a compliance audit of the standard's requirements, the Regional Entity reviews and makes a determination as to whether the actions taken by the Registered Entity were warranted.
Group
SERC EC Planning Standards Subcommittee
Jim Kelley

PowerSouth Energy Cooperative
Yes
Yes
The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers.
Individual
John Tolo
Tucson Electric Power
Yes
Yes
I appreciate the fact that there is a review of the NERC Standards as well as a review of the absolute need for various Standards and/or requirements. I also appreciate that the regulatory bodies are agreeable to such changes and improvements to the compliance process.
Group
Salt River Project
Bob Steiger
ERC Department of Salt River Project
Yes
We like the criteria and methodology.
Yes
Yes
No additions at this time.
Individual
paul haase
seattle city light
Yes
Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Yes
Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Individual
Thad Ness
American Electric Power
Yes
No
AEP does not disagree with a majority of the requirements proposed by the drafting team, though we recommend the team reconsider the inclusion of CIP-003 R3 and associated sub-requirements. AEP recommends instead that CIP-003 R1 be removed in which case CIP-003 R3 (and CIP-003 R2.4) can also be removed. However, if the drafting team does not agree with this recommendation, CIP-003 R3 must be retained in order for entities to take targeted exception(s) where applicable (for example,

in circumstances where an entity's program is more stringent than the CIP requirements). AEP would like the team to consider the following additional Reliability Standard requirements as candidates for retirement on this initial, or subsequent, request for comment. Standard: PRC-021-1 Requirement: R2 Requirement Text: Each Transmission Operator and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request. Criterion: B4,9 Standard: PRC-018-1 Requirement: R5 Requirement Text: The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years. Criterion: B2 Standard: PRC-016-0.1 Requirement: R3 Requirement Text: The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days). Criterion: B4 Standard: PRC-015-0 Requirement: R3 Requirement Text: The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of Studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days). Criterion: B4 Standard: PRC-011-0 Requirement: R2 Requirement Text: The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days). Criterion: B4 Standard: PRC-007-0 Requirement: R3 Requirement Text: The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days). Criterion: B4 Standard: CIP-006 Requirement: R1.5 Requirement Text: Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4. Criterion: B7 Standard: CIP-007 Requirement: R5.1.1 Requirement Text: The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5. Criterion: B7 Standard: CIP-007 Requirement: R5.1.3 Requirement Text: The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4. Criterion: B7 Standard: CIP-007 Requirement: R6.3 Requirement Text: The Responsible Entity shall maintain logs of system events related to cyber security, where technically Feasible, to support incident response as required in Standard CIP-008-3. Criterion: B7 Standard: CIP-007 Requirement: R6.4 Requirement Text: The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days. Criterion: B1, B3 Standard: CIP-003-3, CIP-003-4 Requirement: R1 Requirement Text: Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following: Criterion: B1, B3, B7, B9 Standard: CIP-003-3, CIP-003-4 Requirement: R1.2 Requirement Text: The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. Criterion: B1, B3, B7, B9 Standard: CIP-003-3, CIP-003-4 Requirement: R1.3 Requirement Text: Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2. Criterion: B5 Standard: CIP-003-3, CIP-003-4 Requirement: R2.4 Requirement Text: The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy. Criterion: B7 Comment: Although AEP does not necessarily agree with removal of this requirement (see R3 comment below), R2.4 is redundant with R3.3 (which is being removed) and should probably be removed along with R3. Standard: CIP-003-3, CIP-003-4 Requirement: R3 (R3.1, R3.2, R3.3) Requirement Text: Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). Criterion: Comment: If R1 is not removed, R3 (or some exception process) is necessary. For example, if the Cyber Security Policy goes above and beyond the standards, then an exception may be needed even though the standards are met.
Please see the response to Question #2 for additional Reliability Standard requirements that AEP would like to be considered as candidates for retirement on this initial, or subsequent, request for comment.
While AEP supports the efforts of this drafting team, it might have been advantageous to first agree on the criteria as a first phase, and then once determined, enter a second phase where requirements

were proposed based upon the agreed-upon criteria. This might enable the fast-tracking of the criteria to be used by other concurrent projects and project teams.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Southwest Power Pool Regional Entity
Yes
No
SPP RE does not agree that PRC-008 R1 and R2 should be retired or that they provide "little protection to the BES and [are] better handled under event analysis and lessons learned papers". UFLS equipment maintenance and testing programs ARE important to BES reliability, in a preventative mode, and are NOT covered under the Event Analysis process. Preventative maintenance is very important to reliability; without it, events are more likely. Industry should not wait for an event to happen to collect information and consider maintenance and testing. UFLS is the last line of "defense in depth protection of the BES" (Criteria C6). SPP RE's comment follows the discussion around removing PRC-005 and its relationship to BES reliability. SPP RE does not agree that CIP-007-3 R7.3 should be retired. R7.3 requires the Responsible Entity to maintain records of how data storage media was erased or destroyed prior to disposal or redeployment of the Cyber Asset (which could be simply the media previously removed from the Cyber Asset). In the absence of such records, the Responsible Entity cannot demonstrate compliance with CIP-007-3 R7.1 and CIP-007-3 R7.2, rendering those requirements not auditable. Elimination of this requirement could also result in a loss of visibility of Cyber Assets that have been disposed of or redeployed, also hampering the ability of the Responsible Entity to demonstrate compliance and the Compliance Enforcement Authority to audit compliance with the remaining requirements.
Individual
John Seelke
Public Service Enterprise Group
Yes
No
For these requirements, KEEP: CIP-001-2a R4. If the entity owns or operates a BES asset, there is a clear reliability benefit to have appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to these Law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response. Thus we feel that this requirement should be kept within the standards. CIP-003-3 R3. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. It's removal may have a negative impact on the industry. CIP-003-4 R3. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. It's removal may have a negative impact on the industry. TOP-005-2a R1. "TOP-003-2 requires operating entities such as GOs and TOs to provide operating data to BAs ands TOPs. In TOP-005-2a, R2 and R3 requires BAs and TOPs to exchange this data with other BAs and TOPs . R1 requires BA and TOP recipients of such data to execute a confidentiality agreement so that its confidentiality is protected. This requirement ultimately protects the confidentiality of data provided by entities under TOP-003-2. For these requirements, KEEP BUT MODIFY: FAC-002-1 R2. We believe the three year limitation on documentation sets a limit; otherwise six years may be required (the period between audits. We do suggest removing the language " and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days)." because we see no reliability benefit. For these rerquirements, KEEP UNTIL REPLACED: EOP-

004-1 R1. NERC's Event Analysis Process was approved by NERC's BOT on February 9, 2012. This process has already been adopted as RFC's process under EOP-004-1, R1. Draft standard EOP-004-2 will replace Regional reporting requirements in R1 with consistent NERC-wide requirements; however, while the draft does not presently require the use of the NERC Event Analysis Process, that process is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. Keep until these NERC ROP changes are approved by FERC and become effective. PRC-008-0 R1. This is required for reliability. Such a testing program has been incorporated into draft PRC-005-2 When this is adopted, PRC-008-0 can be retired. PRC-009-0 R1. The NERC Event Analysis Process is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. Keep until these NERC ROP changes are approved by FERC and become effective. PRC-009-0 R1.1. See R1 above. PRC-009-0 R1.2. See R1 above. PRC-009-0 R1.3. See R1 above. PRC-009-0 R1.4. See R1 above.
Individual
Jose H Escamilla
CPS Energy
Yes
Yes
No additional comments.
No additional comments.
Group
Bonneville Power Administration
Chris Higgins
Transmission Reliability Program
Yes
No
BPA does not support the proposed retirement of TOP-001-1a R3. BPA does not agree that TOP-001-1a R3 is redundant with IRO-001-1a R8 because IRO-001-1a R8 only addresses RC directives, whereas TOP-001-1a R3 addresses both RC directives and TOP directives. BPA believes that retiring TOP-001-1a R3 before TOP-001-2 R1 is effective would create a gap because no requirement would address TOP directives. BPA supports the additional proposed retirements and thanks the drafting team for their efforts.
Group
Dominion
Connie Lowe
Dominion
Yes
Yes
In the Complete Set of Standards with Proposed Retirements for Phase 1 pdf; Need to add IRO-001-1a R8 and MOD-004-1 R8 needs to be completely highlighted. In the Spreadsheet with Proposed Retirements; Suggest the MOD-004-1 Requirements be put in numeric order. Need to add IRO-001-1a R8; it is not listed on the spreadsheet.
Individual

Laura Lee
Duke Energy
Yes
Yes
The initial phase of the P81 project should contain only requirements that can quickly gain industry and regulatory support and that there is adequate time to prepare a strong technical justification for. Duke Energy asks the P81 Standards Drafting Team to ensure these parameters are taken into consideration as the list is finalized, and move to a subsequent phase any requirements that could take additional time to develop a strong technical justification and consensus for.
Duke Energy generally supports the comments submitted by The Edison Electric Institute (EEI) and the process being used to respond to the Commission's invitation in the FFT Order.
Group
SPP Standards Review Group
Robert Rhodes
Southwest Power Pool
Yes
We concur that the proposed criteria are a good starting point for the evaluation of requirements to be retired.
Yes
From our review of the list we feel that this is again, a good starting point, but would hope that the drafting team could add or subtract requirements as needed as Phase 1 of the project develops.
VAR-002 R3 Status changes on AVRs – Quite often status changes to AVRs may be made for only a matter of seconds. These changes do not impact the reliability of the BES but still require a call be made for notification of the change. Perhaps the requirement could be changed such that only status changes which impact the BES need to be reported. This hits on Items 4, 5, 8 and 9 in Criterion B. FAC-003-1 R1.3 – Specific training is required for personnel involved with vegetation management programs. This requirement is purely administrative (Criterion B.1) and does not, in and of itself, benefit the reliability of the BES. (Although this requirement has been removed in subsequent versions of this standard (FAC-003-2 and FAC-003-3), it remains in effect today. It needs to be retired.) While we don't have an extensive list at this time, we would hope that the drafting team will ask for potential candidates which fit this category at some point in the future prior to the start of work on the latter phases of the project.
The following are typos we found in the SAR: Either delete the 'an' or make 'processes' singular in Technical Criteria B.2.(b). Either delete the 'that' in the 5th line or the 'to' in the 6th line of the Statement paragraph under CIP-001-2a R4. This is the 3rd sentence in the paragraph. Insert an 'a' between 'require' and 'new' in the last sentence of the Statement paragraph under CIP-003-3, -4 R4.2.
Individual
Rich Salgo
NV Energy
Yes
We agree with the Overarching Criterion and the specific Technical Criteria, and believe that the types of requirements specified in the Technical Criteria can be eliminated without any impact to reliable operation of the interconnected transmission system.
Yes
Our review of the rationale for each of the suggested requirements of the draft SAR supports the conclusion that these requirements should be subject to retirement.
We commend NERC and the Drafting Team on their efforts thus far in this important initiative. This process will serve to better focus the industry's limited resources on activities that are necessary for reliability.

Individual
John Falsey
Edison Mission Marketing & Trading
Yes
Yes
Individual
Bob Thomas
Illinois Municipal Electric Agency
Yes
Yes
IRO-010-1a R3
Illinois Municipal Electric Agency fully supports this initiative by the collaboration group which suppports NERC's application of a risk-based focus to it's programs, and which is consistent with SPIG Recommendation 4.
Individual
Michelle R. D'Antuono
Occidental Energy Ventures Corp.
Yes
Occidental Energy Ventures Corp. ("OEVC") fully supports the efforts taken by the Trades, NERC, and the Regional Entity Management Group to develop the criteria to identify requirements that may be eligible for retirement and modification. The overarching criterion is extremely important in our view, as it serves to remind us all that FERC's original purpose as defined by Section 215(a)(4) of the Federal Power Act is to oversee wide-area reliability of the bulk power system. In recent years, the Commission's authority has expanded into distribution systems and localized load shedding – important issues, but already regulated by the PUCs. In our view, this is duplicative work that increases costs without serving improved reliability. OEVC also believes that the technical criteria are appropriate and complete for now. However, in our view, Item #8 "Hinders the protection or reliable operation of the BES" and Item #9 "Little, if any, value as a reliability requirement" will need further refinement in future phases of this project. Both are quite subjective, and FERC in our opinion will only respond to fact-based quantitative data that shows that BPS reliability is not improved by a given reliability requirement. A painful reminder may be the requirement for secondary Facility Ratings (FAC-008-3) which FERC clearly perceives to be a reliability imperative despite overwhelming industry rejection of the concept. It is unlikely that this view will change unless tangible cost/benefit evidence to the contrary is provided to the Commission.
Yes
OEVC believes that the phased approach proposed in the SAR is prudent and likely the most effective. Only the most obvious candidates for retirement or modification should be presented at this early date. If the industry moves too-far, too-fast, the result may be a blanket rejection of every proposal. Once FERC is comfortable that the industry is in-tune to their sense of risk – which includes public perception of their oversight effectiveness – we believe they will be prepared to deal with requirements that seem important on the surface, but whose contribution to reliability is illusory.
OEVC agrees with the process that the Trades are using to approach this question, but do not agree with some of their priorities. OEVC has only addressed the Requirements where OEVC has additional comments to what the Trades have provided. In addition, OEVC believes the following requirements can also be removed: a) BAL-005, R1.1 – BA metering is financial in nature. Telemetry is already required for reliability. b) TOP-002, R13 – Generator validations are driven by the regions already. FAC-001-0 (all requirements) Criteria B 1, 3 and 6 Statement: OEVC agrees with the Trade's analysis.

but will also point out that once connection requirements are in place, they will rarely change. We believe this would mean a lower priority is in order. All INT Standards Criteria B 6, 7 and 9 Statement: Again, OEVC agrees with the Trades on this. It may even be time to suggest that the functional designation of the PSE go away. They serve a marketing purpose and are blind to reliability indicators. All data collection requirements not included in the Initial Phase CIP-005-3a, -4a R5.3 CIP-006c, -4c R7, R8.3 CIP-007-3, -4 R5.1.2; R6.4; R7.3 CIP-008-3, -4 R2 PRC-018-1 R5 Criteria B 1, 2 and 9 Statement: OEVC agrees with the Trades. Most of these are captured in Phase I. These fit in the same category. All reporting out requirements not included in the Initial Phase CIP-001-2a R3 should be modified to eliminate the word “reporting” (added by OEVC) EOP-002-3 R9.2 EOP-004-1 R3 and its sub requirements; R4 and R5 FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4 FAC-010-2.1 R5 FAC-011-2 R5 FAC-013-2 R6 MOD-010-0 R2 Similar to MOD-012-0 (added by OEVC) MOD-012-0 R2 MOD-020-0 R1 MOD-021-1 R3 PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3. PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2 TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2. Criteria B 1, 4 and 9 Statement: In addition to the Trade’s comments, OEVC believes that NERC has an Events Analysis process, RAPA process, and Section 1600 Data Request process that they can invoke to get this information. Annual reviews CIP-002-2, -4 R4 CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3 CIP-006-3c, -4 R1.8 CIP-007-3, -4 R9 CIP-009-3, -4 R1 EOP-005-1 R1; EOP-005-2 R3.1 EOP-008-0 R1.7 EOP-008-1 R5 IRO-014-1 R4.3 Criteria B 1, 2, 3, 7 and 9 Statement: OEVC agrees with the Trades and add that Compliance teams spend far too much time trying to confirm that a RBAM was reviewed and signed off-on. This serves only to add time and expense – especially when conditions have not changed in the preceding year. Other requirements EOP-004-1 R2 Criteria B 7 Statement: OEVC agrees with the Trades. Again, NERC has an Events Analysis process and RAPA process that they can invoke to require analyses. FAC-002-1 R1 OEVC agrees that this requirement and five sub-requirements are unnecessary. First of all, the PUC, the BA, and the TOP are highly involved in the interconnection process. It is not clear what extra value is provided by overlapping oversight from the RE and/or NERC. Second, other standards – the TPLs in particular – are directly referenced in the requirement. Those are enforceable already, there is no need to duplicate them here. FAC-008-1 R1.3.5 This requirement is already addressed in Phase I. IRO-001-1.1 R8 OEVC believes the intent is to consolidate RC directives in IRO-001 with TOP directives in TOP-001. Since Phase I addresses TOP-001, this seems to have been already accomplished. IRO-005-3a R10 Criteria B 9 Statement: OEVC agrees with the Trades. This is one that we propose should be a much higher priority. Since the GOP is already told to follow a directive, this requirement makes no sense. MOD-017-0.1 R1.1 and MOD-018-0 (all requirements) ; MOD-020-1 R1 OEVC believes that this is redundant with IRO-010 and the new version of TOP-003 when it takes effect. MOD-019-0.1 R1 OEVC believes that this is redundant with IRO-010 and the new version of TOP-003 when it takes effect. TOP-002-2b R2; R15 OEVC believes that TOP-002 R15 will be resolved by the release of the new TOP standards. TOP-002-2b R14 and R14.1 Criteria B 9 Statement: OEVC believes that TOP-002 R14 and R14.1 will be resolved by the release of the new TOP standards. TOP-003-1 R1 and its sub requirements; R2 and R3 Criteria B 9 Statement: OEVC believes that these items will be resolved by the release of the new TOP standards. TOP-005-2a R3 Criteria B 9 Statement: OEVC agrees with the Trades on this one. Again, it may even be time to suggest that the functional designation of the PSE go away. TOP-006-2 R1.1, R4, R5, R6; TOP-008-1 R2, R4 OEVC believes that that TOP-006 R1.1 will be resolved by the release of the new TOP standards.
OEVC Agrees with the Trade Associations on this response.
Individual
Patrick Brown
Essential Power, LLC
Yes
No
CIP-001-2a, R4. This requirement should be removed from the Paragraph 81 project. If an entity owns or operates a BES asset, there is a clear reliability benefit to have appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to

these law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response. Thus we feel that this requirement should be kept within the standards. CIP-003-3, R3. This requirement should be removed from the Paragraph 81 project. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform to its cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. Its removal may have a negative impact on the industry. CIP-003-4, R3. This requirement should be removed from the Paragraph 81 project. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform to its cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. Its removal may have a negative impact on the industry. EOP-004-1, R1. This requirement should be removed from Phase 1 of the Paragraph 81 project, until replaced by EOP-004-2. NERC's Event Analysis Process was approved by NERC's BOT on February 9, 2012. This process has already been adopted as RFC's process under EOP-004-1, R1. Draft standard EOP-004-2 will replace Regional reporting requirements in R1 with consistent NERC-wide requirements; however, while the draft does not presently require the use of the NERC Event Analysis Process, which is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. This requirement should be kept until these NERC ROP changes are approved by FERC. FAC-002-1, R2. This requirement should be removed from the Paragraph 81 project, and modified instead. We believe the three year limitation on documentation sets a limit; otherwise six years may be required (the period between audits). We do suggest removing the language “and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days)." because we see no reliability benefit to this element of the requirement.
Individual
Becky Stewart
Idaho Power Company
Yes
Yes
MOD-017-0.1 R1.1, R1.2 Criterion B2 MOD-018-0 R1 Criterion B7 (Should be covered by MOD-016) MOD-021-1 R1, R2 Criterion B7 (Should be covered by MOD-016) MOD-021-1 R3 Criterion B4
MOD standards 016 through 021 should be combined into a single standard, removing duplication and retiring requirements which are "reporting-only" and/or have little discernable reliability benefit. We agree with the stated Purpose or Goal of the proposed standard of setting forth specific Reliability Standard requirement evaluation criteria and establishing a multi-phased process for addressing these Reliability Standard requirements. We agree with and support this Reliability Standard requirement evaluation and proposed multi-phased process based on the following: We believe there is value in differentiation of violations based on risk. We believe that not all violations pose the same risk to reliability, so they should not all be treated the same. Focusing on the greatest risks to reliability will allow for more efficient use of resources while improving the reliability of the BES through an application of structured risk management.
Group
Pepco Holdings Inc & Affiliates
David Thorne
Pepco Holdings Inc
Yes
Yes
Pepco Holdings Inc supports this project. Additionallyl Pepco Holdings Inc supports the comments provided by EEI.

Individual
Kimberly Tolbert
Occidental Power Services, Inc.
Yes
No
OPSI recommends the following additions for Phase 1 implementation: 1. INT-001-3, R1. The Load Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour. Criteria: B6, B9 Statement: This requirement is at best a business practice of markets (protocol). These schedules can be rejected if not correctly submitted, can be cut if not executed correctly, and the PSE can be penalized if there are offenses. Recommendation: Remove PSE from R1 and from the Applicability section. 2. INT-004-2, R2. The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs: o R2.1 The average energy profile in an hour is greater than 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than ±10% o R2.2 The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than ±25 megawatt-hours o R2.3 A Reliability coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons. Criteria: B6,B9 Statement: This requirement is at best a business practice of markets (protocol). These schedules can be rejected if not correctly submitted, can be cut if not executed correctly, and the PSE can be penalized if there are offenses. Recommendation: Remove PSE from R2 and from the Applicability section. 3. IRO-001-1.1, R3 and R8. R3. The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing- Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes. R8. Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions. Criteria: B9 Statement: PSEs do not generally receive Reliability Directives from RCs Recommendation: Remove PSE from R3 and R8 and from the Applicability section. 4. IRO-005-3, R10. In instances where there is a difference in derived limits, the Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall always operate the Bulk Electric System to the most limiting parameter. Criteria: B9 Statement: PSEs do not generally derive limits for the transmission of power over the BES. Recommendation: Remove PSE from R10 and from the Applicability section. 5. TOP-005-2, R3. Each Purchasing-Selling Entity shall provide information as requested by its Host Balancing Authorities and Transmission Operators to enable them to conduct operational reliability assessments and coordinate reliable operations. Criteria: B6,B9 Statement: PSEs have to supply this information as a requirement for participating in market functions. Recommendation: Remove PSE from R3 and from the Applicability section. 6. VAR-001, R5. Each Purchasing-Selling Entity shall arrange for (self-provide or purchase) reactive resources to satisfy its reactive requirements identified by its Transmission Service Provider. Criteria: B6,B9 Statement: This is a requirement to participate in competitive markets (generally, it is included in the transmission rate) or is required by tariffs in non-competitive markets. The PSE has no option but to purchase the reactive power in order to make the transaction. Recommendation: Remove PSE from R5 and from the Applicability section.
If the changes listed in Question 2 are not considered in Phase 1, then they should be considered in subsequent phases of the project.

Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
Yes
FAC-001-0 (all requirements) Criteria B 1, 3 and 6 Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. Once an interconnection request is actually made with a transmission owner, the transmission owner performs the FAC-002-1 steady-state, short-circuit, and dynamics studies to determine the new interconnection's impact on reliability. During the negotiation of an interconnection agreement the FAC-001-0 referenced material is agreed on and reduced to writing for purposes of constructing, maintaining and operating the interconnection facilities. Also, during the entire interconnection process, as FAC-002-1 provides for, the parties must coordinate and cooperate during the assessment of the reliability impact of the new interconnection facilities. Thus, FAC-001-0, at best, is a best practice or helpful initial guide to an entity considering interconnecting, but provides little, if any, meaningful value to reliability, especially when compared to the actual benefits to reliability via the FAC-002-1 studies, the execution of a negotiated agreement and the coordination of activities during constriction and operation of the new facilities. Accordingly, FAC-001-0 should be retired, and, if necessary, any requirements that protect reliability should be transferred to FAC-002-1. All INT Standards Criteria B 6, 7 and 9 Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Thus, we recommend that the Standards Drafting Team retire the INT Reliability Standards and, as necessary, transfer any requirement that protect reliability to the BAL Reliability Standards. All data collection requirements not included in the Initial Phase, more specifically: CIP-005-3a, -4a R5.3 CIP-006c, -4c R7, R8.3 CIP-007-3, -4 R5.1.2; R6.4 CIP-008-3, -4 R2 PRC-018-1 R5 Criteria B 1, 2 and 9 Statement: These requirements are purely data retention requirements with no functional nexus to reliability and, therefore, best handled via compliance monitoring, RSAW or as a data request during an audit. All reporting out requirements not included in the Initial Phase, more specifically: EOP-002-3 R9.2 EOP-004-1 R3 and its subrequirements; R4 and R5 FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4 FAC-010-2.1 R5 FAC-011-2 R5 FAC-013-2 R6 MOD-012-0 R2 MOD-020-0 R1 MOD-021-1 R3 PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3. PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2 TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2. Criteria B 1, 4 and 9 Statement: There is no direct connection between reporting out of information to an entity or Regional Entity and protecting reliability. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards. Annual reviews CIP-002-3, R3; CIP-002 -4 R3 CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, -4 R5.1.2; CIP-003-3, - 4 R5.3 CIP-006-3c, -4 R1.8 CIP-007-3, -4 R9 CIP-009-3, -4 R1 EOP-005-1 R1; EOP-005-2 R3.1 EOP-008-0 R1.7 EOP-008-1 R5 IRO-014-1 R4.3 Criteria B 1, 2, 3, 7 and 9 Statement: The annual review and update requirements are arbitrary, administrative and not aligned with the operation and protection of the Bulk Electric System. These requirements should be retired or modified to align with how the Bulk Electric System is operated and protected. Other requirements CIP-007-3, -4 R7 Criteria B 1, 2, 3 and 7 Statement: The essential elements of the process of disposing or redeploying of Cyber Assets and the associated cyber security are set forth in R7.2 and R7.3. To require "formal methods, processes and procedures" appears to require formal documentation for the sake of documentation, rather than allowing the responsible entity to implement a process that achieves the actions required in R7.2 and R7.3, which may or may not include formal procedures, for example. EOP-004-1 R2 Criteria B 7 Statement: The analysis of the BES for system disturbances is covered in PRC-004-2.1a R1. The PRC Requirement R1 calls for the analysis of its transmission Protection System Misoperations. We believe that BES analysis is covered inherently through this PRC standard making EOP-004 R1 redundant to the PRC standard. Another

factor is the Version 2 of the EOP-004-2 where the requirement to analyze the BES disturbance is noticeably absent. The focus on the EOP-004 is for the reporting of applicable events that are identified in the PRC-004 standard. There is an event analysis reporting process referenced in the NERC Rules of Procedures (ROPs) that handles this requirement. Therefore, this is a redundant requirement. In February of 2012, NERC deployed its Events Analysis Process – incorporating the learnings from two field trials held over the previous year and a half. It includes all the necessary steps that affected operators must take to analyze and report on events that may impair the reliability of the BES. Most Regional Entities have already updated their reporting procedures to match NERC's. Furthermore, NERC and the Regional Entities already have sufficient authority to order analyses and corrective action plans outside of the Reliability Standards. These are important steps for the development of Lessons Learned and trending analyses, but do not contribute to reliable operations. In fact, the demand for near term reporting – some within one hour of the initiation of the event – interferes with the efforts of front-line personnel to mitigate the issue at hand BAL-001-0.1a (all requirements), BAL-004-0 (all requirements), BAL-005-0.1b R11; BAL-006-2 (all requirements) Criteria B 6 and 9 Statement: BAL-001 requires a 12 month rolling average of ACE and does not impact reliability and should be eliminated (in favor of BAL-002). Consider augmenting NAESB standard WEQ-005. BAL-004 requirement for time error correction is not important for reliability and should be eliminated. It also duplicates NAESB std WEQ-006. In BAL-005 R11, Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE, is not needed for reliability. Ramp rates have minimal impact on ACE calculations, and are already included in the definition of Interchange Schedule in the NERC Glossary as used in R9. The requirement to use agreed upon ramp rates is commercial in nature and is already covered by NAESB standard WEQ-004-17. BAL-006-2 is an after-the-fact accounting of inadvertent interchange and does not impact reliability and should be eliminated. Consider augmenting NAESB standard WEQ-007. CIP-003-3, -4 R2 and its subrequirements Criteria B 1 and 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is an employee called a CIP senior manager oversees the plan. CIP-004-3, -4 R2.3 Criteria B 9 Statement: Whether the entity has a robust up-to-date, trained-on CIP compliance plan may impact reliability, but not whether there is annual training. CIP-004-3, -4 R3.2 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is a seven year update to the PRA. CIP-004-3, -4 R4.1 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it reviews lists every seven days. CIP-004-3, -4 R4.2 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it revokes access within 24 hours or 7 days. CIP-005-3a, -4a R2.5 and its subrequirements Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the ESP may impact reliability, but not whether specific information is documented. CIP-007-3, -4 R3.1, R3.2 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented within 30 days. Also, whether the entity has a robust up-to-date on CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented. CIP-008-3 R1.4 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether specific information is documented within 30 days or a change. EOP-001-1b, -2b Criteria B 7 Statement: Duplicative with the other EOP Standards (e.g., Capacity and Energy emergency of EOP-002, Load Shedding of EOP-003, and System Restoration of EOP-005). EOP-002-3 R1 Criteria B 7 Statement: Duplicates other requirements such as IRO-001-1 R8 and should be retired or modified to reduce redundancy. EOP-002-3 R9 Criteria B 7 Statement: When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources). It duplicates NAESB standard WEQ-008 and should be eliminated. EOP-005-2 R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration. Criteria B 1, 3 and 7 Statement: With the implementation of NUC-001-2 R2, there is no longer a need for EOP-005-2 R1.2. Specifically, NUC-001-2 R2 requires Nuclear Plant Interface Requirements (NPIRs) to be included in the agreements for operation and maintenance (including restoration process) for off-site nuclear power: R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more

Agreements1 that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. Given the off-site power requirements of NUC-001-2 which require comprehensive operational interface protocols (including restoration) between nuclear plants and responsible entities as part of the NPIRs, there is no longer a need for the administrative, documentation-only requirement in EOP-005-2 related to the same subject matter. IRO-002-2 (all requirements) Criteria B 7 Statement: Redundant with COM-002-2, R1 COM-001-1.1, R1 and IRO-002-2, R2 and R3 IRO-005-3a R10 Criteria B 9 Statement: Confusing requirement. It was intended to address rare cases where entities were told to operate to different SOLs and IROLs. However, because only the TOP and the RC can see these parameters, the only thing a GOP can do is follow a directive. IRO-014-1 R4 Criteria B 9 Statement: Requirement 4 (including sub-parts) should be rolled up into R1. and eliminated. Requirement 1 should be modified to require "current operating procedures, processes or plans with all adjacent RCs. IRO-015-1 R2.1 Criteria B1 and 9 Statement: Whether the procedure, process and plan is robust and up-to-date may impact reliability, not whether there are weekly calls. MOD-001-1 and MOD-008-1 (all requirements) Criteria 6 and 9 Statement: Do the ATC / TTC standards belong in NERC or NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? I think NERC should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., and I think these can/should be moved to the NAESB standards. Criteria B 6 and 9 Statement: This could be handled as a data request from an RE or other Registered Entities and, therefore, would not need a requirement, as there are too many requirements that warrant an attestation that no request was made. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9 Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard. MOD-028-1 (all requirements); MOD-029-1a (all requirements); MOD-030-2 (all requirements) Criteria B 6 and 9 Statements: ATC / TTC standards should belong NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? NERC should focus on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc. PRC-022-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.5 Criteria B 7 Statement: Whether the responsible entity has robust UVLS misoperation and correction action is redundant with PRC-004-1a, -2a. TOP-001-1a R3 and R7 (and its subrequirements) Criteria B 9 Statement: For R3, there are three projects in progress addressing the issuance of directives by the RC, BA and TOP. Also, for R7, all outages information should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-002-2b R8 and R 9 Criteria B 6, 7 and 9 Statement: “Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency”, duplicates VAR-001 and should be eliminated. “Each Balancing Authority shall plan to meet Interchange Schedules and ramps” duplicates the BAL standards and the NEASB standards and should be eliminated. TOP-002-2b R12 Criteria B 6 and 9 Statement: ATC / TTC standards should belong to NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12). NERC should focus on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., These can/should be moved to the NAESB standard. TOP-002-2b R14 and R14.1 Criteria B 9 Statement: All derating information should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-002-2b R15 Criteria B 9 Statement: Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations is a "how" requirement that is needed to meet other requirements in the standard. It is also not measureable, and the requirement should be eliminated. All weekly forecasts should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-003-1 R1 and its subrequirements; R2 and R3 Criteria B 9 Statement: All planned outage information should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-005-2a R3 Criteria B 9 Statement: PSEs are not best positioned to provide reliability information. BAL-005-0.1b R1 Criteria B7 Statement: Introductory statement; redundant with subrequirements MOD-010-0 R2 Criteria B 1, 4 and 9 Statement: MOD-012-0 R2 was included in the Joint Trade Associations list of suggested requirements for retirement or modification. MOD-010-0 R2 is nearly identical to MOD-012-0 R2 and should also be considered. PER-001-0.1 R1 Criteria B7 Statement: The TOP portion of this requirement is redundant with TOP-001-1a R1 PRC-018-1 R3 (and all sub requirements) Criteria B2 and 4 Statement: This requirement involves data collecting and reporting that does not impact the reliability of the BES; could be part of a data request if necessary

The P81 project should be considered a high priority Standards development project for the following reasons: (1) Responsive to P81 of FERC’s March 15, 2012 order and SPIG Recommendation No. 4 (2)

Will increase efficiency of the ERO compliance programs (3) Requirements submitted for the initial phase appear to be clear candidates on their face and should not require extensive technical research (4) The collaborative nature of the project is an example for future work, because it advances the project while reducing the impact on stakeholders and NERC staff (5) The proposed pace of the project sets an example for future work (6) Furthers the focus on results, performance based Reliability Standards (7) May provide a roadmap of what should or should not be a requirement in future Reliability Standards (8) The draft P81 SAR criteria is designed to be sufficiently broad to capture all FERC approved reliability Standards that are unnecessary, redundant or do little to protect reliability (9) To eliminate Reliability Standards requirements that deter from our focus on reliability Based on these benefits, we support the Standards Drafting Team and NERC staff working together to file the initial list of Reliability Standards for retirement with the Federal Energy Regulatory Commission prior to the end of the year and that the Standards Drafting Team also make significant progress on the scope of the phase two P81 Reliability Standards list by the end of the year.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
I support removing redundancy and any items that are not related to reliability impacts.
Yes
Will the measures associated with requirements that are up for retirement be modified or removed? Eg. Removing R2 of a standard but not removing the text in M1 which refers to R2 of that same standard.
Instead of retiring R2 of EOP-009-0 could the whole standard can be replaced by the new EOP-005?
Individual
Eric Olson
Transmission Agency of Northern California
Yes
Yes
TANC commends FERC for soliciting input on ways to eliminate requirements that are redundant or provide little protection for the bulk power system. TANC believes that NERC has proposed an appropriate response to this opportunity and looks forward to further initiatives that prioritize reliability ahead of compliance.
Group
ACES Power Marketing Standards Collaborators
Jason Marshall
ACES Power Marketing
Yes
In general, we agree with the criteria. However, we do offer two suggestions. First, in criterion B.1, we suggest striking “and is needlessly burdensome”. If the activity does not support reliability the burden is irrelevant. Second, we suggest if there are current standards under development that are already proposing to retire requirements that those requirements should be considered for inclusion in this project. In order to include those requirements, the proposed reason for retirement should align with one of the criteria in this project. This would accelerate the retirement of unnecessary requirements. Third, we suggest requirements that are assigned to the wrong functional entities should be added as a criterion for revision/retirement.
No
(1) We believe there are other requirements that easily meet the criteria. (2) VAR-001-2 R5 is redundant with FERC’s pro forma tariff and was originally included in the NERC policies to align them with said tariff. The requirement compels the PSE and LSE to arrange for reactive resources to satisfy

the reactive requirements of the Transmission Service Provider. PSEs and LSEs cannot purchase transmission service without purchasing reactive service or demonstrating to the transmission provider that they have arranged for reactive resources. From a practical perspective, this means they always purchase reactive service from the Transmission Provider. Furthermore, it is the Transmission Operator that actually ensures reactive resources are dispatched per VAR-001-2 R2. Thus, VAR-001-2 R5 satisfies criteria B.1, B.6, B.7, and B.9. (3) BAL-002 R1 and R3 are redundant. R1 compels the BA to have access to and operate Contingency Reserve to respond to disturbances. R3 requires the BA to activate sufficient Contingency Reserve to comply with DCS. We suggest removing R1 because it is redundant (Criterion B.7). This applies to both versions 0 and 1 of the standard. (4) BAL-005-0.1b R1 and its sub-requirements are not necessary. All generation, transmission and load is currently contained within the metered boundaries of a BA. It is impossible to add new generation, transmission and load and not be within the metered boundaries of a BA. To do so, would require the equipment owner to carve out an area from the BA. For example, if a TO added a new transmission line, it would have to put a meter on both ends to carve it out of any BA footprint. In the process, they, in effect, create a new BA. The only way these requirements can't be met would be if BAs started removing metering equipment en masse. Given removing metering equipment has significant financial consequences due to inaccurate energy accounting; it is not going to happen. Thus, it meets Criterion B.9. Furthermore, TOs are already required to identify metering requirements in FAC-001-0 R2.1.6 as part of its facility connection requirements. It also meets Criterion B.7. (5) COM-001-1.1 is unnecessary and the audit of it has largely become a demonstration that it is an administrative requirement. English is the primary language across the vast majority of the Interconnections under NERC's purview and it is the primary language in all of the areas under FERC's jurisdiction. For the few companies in areas where English is not predominant, those companies will be unable to meet other requirements if they use a different language to speak with companies from predominantly speaking English languages. Furthermore, audits have regulated this to predominantly an administrative requirement. The auditors largely look for statement that the English language is required despite the fact that all evidence has been provided in English, observations of control center conversations have shown English is used, and the audit has been conducted in English. If there is a need for this requirement, it should be relegated to a regional requirement for those regions that include areas that do not speak predominantly English. Thus, this requirement meets Criteria B.1 and B.9. (6) FAC-010-2.1 R5 is an administrative requirement for the Planning Authority to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The PC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments. This requirement meets Criteria B.1 and B.9. (7) FAC-011-2 R5 is an administrative requirement for the Reliability Coordinator to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The RC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments when they receive the methodology. This requirement meets criteria B.1 and B.9. (8) INT-004-2 R1 has nothing to do with reliability and should be included in the list of retirements. Failing to reload an Interchange Transaction that was curtailed for a reliability event has no reliability impact. It is a remnant from the NERC Policies that was added at the request of market participants because once transactions were cut, reliability entities did not always allow the transaction to resume once the reliability issue had been addressed. This is strictly a commercial issue. Thus, this requirement meets Criterion B.9. (9) IRO-005-3 R10 should be modified to reflect the functional model. In cases where there are differences in derived limits, PSEs and LSE cannot operate to the most limiting parameters. They are not in a position to even have information on the parameters such as facility ratings. Rather, their role is to follow directives. Thus, inclusion of PSE and LSE in the requirement does not support reliability. Thus, this requirement meets Criterion B.9. (10) IRO-005-3 R11 is redundant with MOD-028-1 R6.1, MOD-029-1a R3, and MOD-030-2 R2.4. The MOD standards already require the TSP to consider IROLs and SOLs when determining Available Transfer Capability/Available Flowgate Capability and Total Transfer Capability. This requirement meets Criterion B.7. (11) PRC-011-0 R2 should be retired. A requirement is not needed to compel the TO and DP to provide data on its UVLS equipment maintenance program to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9. (12) PRC-015-0 R3 should be retired. A requirement is not needed to compel the TO, GO and DP to provide data on their Special Protection Systems (SPS) to the Regional Entity. The

Regional Entity's CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9. (13) PRC-016-0.1 R3 should be retired. A requirement is not needed to compel the TO, GO and DP to provide data on their SPS Misoperations analyses and corrective action plans to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9. (14) PRC-017-0.1 R2 should be retired. A requirement is not needed to compel the TO, GO and DP to provide documentation of the SPS maintenance and testing program to the Regional Entity. The Regional Entities CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9. (15) PRC-021-0.1 R2 should be retired. A requirement is not needed to compel the TO and DP to provide UVLS program data to the Regional Entity. The Regional Entities CMEP and NERC's Rules of Procedure compel the TO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9. (16) PRC-023-1 R2 and PRC-023-2 R3 are redundant with FAC-008-1 R1.2.1 and FAC-008-3 Part 2.4.1. FAC-008-1 R1.2.1 and FAC-008-3 Part 2.4.1 already require the GO and TO to consider relay protective devices when determining facility ratings. The DP cannot limit the Facility Rating because a DP does not have Transmission Facilities. They only have relays that impact Facility Ratings that must ultimately be considered by the TO. This requirement meets Criterion B.7 (17) TOP-005-2a R3 is redundant with the INT standards and should be retired. In the NERC Functional Model, the only role for the PSE is to facilitate Arranged Interchange. The INT standards already govern Arranged Interchange and contain the necessary information that the PSE must provide. Furthermore, Project 2007-03 Real-Time Operations has proposed retirement of this requirement as it is redundant with NAESB e-Tag specifications. Beyond the E-tag data there is no additional information that a PSE or LSE could provide for the BA or TOP to conduct operational assessments. This requirement meets Criteria B.6, B.7 and B.9. (18) PRC-006-1 R7 should be retired. Failure by a Planning Coordinator to provide data to another Planning Coordinator within 30 days is not a reliability issue because Planning Assessments have long time lines to complete the studies. Furthermore, any failure to provide data within 30 calendar days is most likely a simple oversight. If a Planning Coordinator refuses to provide data, the requesting Planning Coordinator may get involved and which will compel them to provide the data. This can be done without the need for this requirement. This requirement meets criterion B.4.

(1) EOP-002-3 R6 and R7 and their sub-requirements are redundant with BAL-001-0.1a R1 and R2 and BAL-002 R4. BAL-001-0.1a R1 compels a BA to meet CPS1. BAL-001-0.1a R2 compels a BA to meet CPS2. BAL-002 R4 compels a BA to respond meet the DCS for all reportable events less than MSSC. EOP-002-3 R6 and R7 do not make the BA any more or less responsible to meet these requirements but rather creates an opportunity for double jeopardy. Furthermore, EOP-002-3 R6 and R7 do not make any sense in context with the CPS1 and CPS2 calculations. They are averages over a long term and would never require the emergency actions listed in the sub-requirements to comply with them. These requirements have already proven to incent behavior that is contrary to reliability (criterion B.8). At the August NERC BOT meeting, the NERC OC Chair explained that a BA shed load to meet the DCS criterion even though there were no other concerns (i.e. voltage, frequency, IROL or SOL violations) on the transmission system at the time. These requirements meet criterion B.7. (2) EOP-004-1 R2 should be considered for future retirement. The approval of the Event Analysis Procedure obviates the need for a standard requirement to analyze Bulk Electric System disturbances. This would be especially true if the procedure is added to the Rules of Procedure as NERC has planned. This requirement meets criterion B.7. (3) Retirement of FAC-001-0 R3 should be considered in the next phase. There is an implied obligation for the TO to update its Facility connection requirements when they change. Additionally, a requirement to make them available to the Regional Entity and users of the transmission system is unnecessary. First, the Regional Entity could request them through the compliance monitoring process. Second, the TO will provide the Facility connection requirements to those with genuine interconnection requests because the TO will want its connection standards met. This requirement meets criterion B.4, B.7 and B.9. (4) FAC-002-1 R1 should be revised to reflect the NERC Functional Model because it assigns the requirements to the wrong functional entities. The Transmission Planner and Planning Coordinator are responsible for conducting the assessments for new Facilities. The requirement appears to be an attempt to require the GO, TO, DP, and LSE to coordinate with the TP and PC. However, the requirement actually defines what is required in the TP and PC assessments which unfortunately place these responsibilities on the GO,

TO, DP and LSE. None of these functional entities have the capability to meet requirements such as performing dynamics studies. This requirement meets criterion B.8. (5) VAR-001-2 R2 and TOP-006-2 R2 are duplicate requirements. VAR-001-2 R2 compels the TOP to acquire sufficient reactive resources. TOP-006-2 R2 requires the RC, TOP and BA to monitor reactive resources. Since VAR-001-2 R2 applies all the time, a TOP cannot know they have acquired and maintained reactive resources unless they are monitoring them. Furthermore, TOP-006-2 R2 incorrectly applies to the BA. According to the NERC Functional Model, the BA cannot monitor reactive resources that are not generators and have no role in ensuring system voltages. Thus, TOP-006-2 R2 meets criterion B.7 because it is redundant, and it meets criteria B.8 and B.9 because it assigns responsibility to a functional entity (BA) that cannot meet it. This distracts the BA from its reliability mission.

NERC needs to develop guidance that includes these criteria for drafting teams to avoid developing requirements that offer little reliability value in the future. There are many standards currently being developed that include similar kinds of requirements that will make a future exercise like this necessary. NERC should expend every effort to avoid such a future situation. Some examples can be found in Project 2007-09 Generator Verification. Proposed MOD-027-1 R3 through R5 largely memorializes the administrative interactions that must occur between the GO and TP to develop a good active power/frequency control model. PRC-004-3 Part 4.2 in Project 2010-05.1 Misoperations is another example. It requires maintenance of data regarding Corrective Action Plans. These are administrative requirements and are unnecessary.

Group

The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade Associations).

Mark S. Gray

Edison Electric Institute

Yes

The Trade Associations agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement. As noted above, the criteria were the product of intense discussions among numerous stakeholders, including the Trade Associations, NERC, and the Regional Entities. The criteria are also consistent with FERC's guidance in paragraph 81 of the FFT Order.

Yes

The Trade Associations agree with the suggested list of Reliability Standard requirements contained in the SAR for the Initial Phase of P81.

The Trade Associations support the following list of Reliability Standard requirements to be retired or modified in a subsequent phase of the P81 project. To assist the Standards Drafting Team decide what should be considered in phase 2, phase 3 etc., the Trade Associations have listed the requirements in the order of importance – with those at the top of the list candidates for phase 2. The Trade Associations understand, however, that the decision on how best to proceed with phase 2, phase 3 will be weighed by the Standards Drafting Team, and, therefore, have not indicated any bright line on what should or should not be included in phase 2 versus phase 3, etc. The Trade Associations further note that the list of requirements listed below may be supplemented with additional requirements as the phase 2/phase 3 discussions evolve. Additionally, the Trade Associations believe that additional criteria for elimination may be proposed as part of the phase 2/phase 3 process. FAC-001-0 (all requirements) Criteria B 1, 3 and 6 Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. Once an interconnection request is actually submitted to a transmission owner, the transmission owner performs the FAC-002-1 steady-state, short-circuit, and dynamics studies to determine the new interconnection's impact on reliability. During the negotiation of an interconnection agreement the FAC-001-0 reference material is agreed on and reduced to writing for purposes of constructing, maintaining and operating the interconnection facilities. Also, FAC-002-1 imposes an obligation on the parties to coordinate and cooperate during the assessment of the reliability impact of the new interconnection facilities. Thus, FAC-001-0, at best, is a best practice or helpful initial guide to an entity considering interconnecting, but provides little, if any, meaningful value to

reliability, especially when compared to the actual benefits to reliability via the FAC-002-1 studies, the execution of a negotiated agreement and the coordination of activities during construction and operation of the new facilities. Accordingly, FAC-001-0 should be retired, and, if necessary, the transfer of any requirements that protect reliability to FAC-002-1. All INT Standards (With the exception of INT-007-1 R1.2 which is part of and should remain in the Initial Phase.) Criteria B 6, 7 and 9 Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Reliability Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Thus, it is recommended that the Standards Drafting Team retire the INT Reliability Standards, and, as necessary, transfer any requirement that protect reliability to the BAL Reliability Standards. ALL DATA COLLECTION REQUIREMENTS NOT INCLUDED IN THE INITIAL PHASE CIP-005-3a, -4a R5.3 CIP-006-3c, -4c R7, R8.3 CIP-007-3, -4 R5.1.2; R6.4 CIP-008-3, -4 R2 PRC-018-1 R5 Criteria B 1, 2 and 9 Statement: These requirements are purely a data retention requirement with no functional nexus to reliability, and, therefore, are best handled via compliance monitoring, RSAWs or as a data request during an audit. ALL REPORTING OUT REQUIREMENTS NOT INCLUDED IN THE INITIAL PHASE EOP-002-3 R9.2 EOP-004-1 R3 and its subrequirements; R4 and R5 FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4 FAC-010-2.1 R5 FAC-011-2 R5 FAC-013-2 R6 MOD-012-0 R2 MOD-020-0 R1 MOD-021-1 R3 PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3. PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2; PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2 TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2. Criteria B 1, 4 and 9 Statement: There is no direct nexus between reporting out of information to an entity or Regional Entity and protecting reliability. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards. Annual reviews CIP-002-3, R3; CIP-002 -4 R3 CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3 CIP-006-3c, -4 R1.8 CIP-007-3, -4 R9 CIP-009-3, -4 R1 EOP-005-1 R1; EOP-005-2 R3.1 EOP-008-0 R1.7 EOP-008-1 R5 IRO-014-1 R4.3 Criteria B 1, 2, 3, 7 and 9 Statement: The annual review and update requirements are arbitrary, administrative and not aligned with the operation and protection of the Bulk Electric System. These requirements should be retired or modified to align with how the Bulk Electric System is operated and protected. OTHER REQUIREMENTS CIP-007-3, -4 R7 Criteria B 1, 2, 3 and 7 Statement: The essential elements of the process of disposing or redeploying of Cyber Assets and the associated cyber security are set forth in R7.2 and R7.3. To require “formal methods, processes and procedures” appears to require formal documentation for the sake of documentation, rather than allowing the responsible entity to implement a process that achieves the actions required in R7.2 and R7.3, which may or may not include formal procedures, for example. EOP-004-1 R2 Criteria B 7 Statement: The analysis of the BES for system disturbances is covered in the PRC-004-2.1a R1. The PRC Requirement R1 calls for the analysis of its transmission Protection System Misoperations. We believe that BES analysis is covered inherently through this PRC standard, making EOP-004 R1 redundant to the PRC standard. Another factor that was considered is the notable absence of any requirement in EOP-004-2 to analyze the BES disturbance. The focus of EOP-004 is on the reporting of applicable events that are identified in the PRC-004 standard. There is an event analysis reporting process referenced in the NERC Rules of Procedures (ROP) that addresses this requirement. Therefore, this is a redundant requirement. In February of 2012, NERC deployed its Events Analysis Process – incorporating the learnings from two field trials held over the previous year and a half. It includes all the necessary steps that affected operators must take to analyze and report on events that may impair the reliability of the BES. Most Regional Entities have already updated their reporting procedures to match NERC’s. Furthermore, NERC and the Regional Entities already have sufficient authority to order analyses and corrective action plans outside of the Reliability Standards. These are important steps for the development of Lessons Learned and trending analyses, but do not contribute to reliable operations. In fact, it is arguable that the demand for near term reporting – some within one hour of the initiation of the event – interferes with the efforts of front-line personnel to mitigate the issue at hand BAL-004-0 (all requirements), BAL-005-0.1b R11; BAL-006-2 (all requirements) Criteria B 6 and 9 Statement: BAL-004 requirement for time error correction is not important for reliability and should be eliminated. BAL-004 also duplicates NAESB standard WEQ-006. BAL-005 R11 states that Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE. This requirement is not needed for reliability. Ramp rates have minimal impact on

ACE calculations, and are already included in the definition of Interchange Schedule in the NERC Glossary as used in R9. The requirement to use agreed upon ramp rates is commercial in nature and is already covered by NAESB standard WEQ-004-17. BAL-006-2 is an after the fact accounting of inadvertent interchange and does not impact reliability and should be eliminated. Consider augmenting NAESB standard WEQ-007. CIP-003-3, -4 R2 and its subrequirements Criteria B 1 and 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is an employee called a CIP senior manager that oversees the plan. CIP-004-3, -4 R2.3 Criteria B 9 Statement: Whether the entity has a robust up-to-date, trained-on CIP compliance plan may impact reliability, but not whether there is annual training. CIP-004-3, -4 R3.2 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is a seven year update to the personnel risk assessment(PRA). CIP-004-3, -4 R4.1 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it reviews lists every seven days. CIP-005-3a, -4a R2.5 and its subrequirements Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the ESP may impact reliability, but not whether specific information is documented. CIP-007-3, -4 R3.1, R3.2 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented within 30 days. Also, whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented. CIP-008-3 R1.4 Criteria B 1, 9 Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether specific information is documented within 30 days or a change. EOP-001-1b, -2b Criteria B 7 Statement: Duplicative with the other EOP Standards (e.g., Capacity and Energy emergency of EOP-002, Load Shedding of EOP-003, and System Restoration of EOP-005). EOP-002-3 R1 Criteria B 7 Statement: Duplicative of other requirements such as IRO-001-1 R8, and should be retired or modified to reduce redundancy. EOP-002-3 R9 Criteria B 7 Statement: When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources). It is duplicative of NAESB standard WEQ-008 and should be eliminated. EOP-005-2 R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration. Criteria B 1, 3 and 7 Statement: With the implementation of NUC-001-2 R2, there is no longer a need for EOP-005-2 R1.2. Specifically, NUC-001-2 R2 requires Nuclear Plant Interface Requirements (NPIRs) to be included in the agreements for operation and maintenance (including restoration process) for off-site nuclear power: Ref: NUC-001-2 R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements1 that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. Given the off-site power requirements of NUC-001-2 which require comprehensive operational interface protocols (including restoration) between nuclear plants and responsible entities as part of the NPIRs, there is no longer a need for the administrative, documentation-only requirement in EOP-005-2 related to the same subject matter. FAC-013-1 (all requirements) Criteria B 6 Statement: It is really a commercial planning practice suitable for Order 1000 under Section 205/206 as opposed to Section 215. IRO-002-2 (all requirements) Criteria B 7 Statement: Redundant with COM-002-2, R1 COM-001-1.1, R1 and IRO-002-2, R2 and R3 IRO-005-3a R10 Criteria B 9 Statement: Confusing requirement. It was intended to address rare cases where entities were told to operate to different SOLs and IROLs. However, since only the TOP and the RC can see these parameters, the only thing a GOP can do is follow a directive. IRO-014-1 R4 Criteria B 9 Statement: Requirement 4 (including sub-parts) should be rolled up into R1 and eliminated. Requirement 1 should be modified to require "current operating procedures, processes or plans with all adjacent RCs. IRO-015-1 R2.1 Criteria B1 and 9 Statement: Whether the procedure, process and plan is robust and up-to-date may impact reliability, not whether there are weekly calls. MOD-001-1 and MOD-008-1 (all requirements) Criteria B 6 and 9 Statement: NERC should be focused on modeling the BES and managing SOLs and IROLs, the methodologies for the determination of CBM, TTC and ATC are commercial matters associated with the reservation and allocation of rights to transfer capability among transmission customers. While transfer capability calculations should be based on models of the BES, the NAESB WEQ should address the issues raised in MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12. Criteria B 6 and 9 Statement: This could be

handled as a data request from an RE or other Registered Entities, and therefore would not need a requirement, as there are too many requirements that warrant an attestation that no request was made. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9 Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard. MOD-019-0.1 R1 Criteria B 1, 2, and 9 Statement: MOD-019-0.1 covers "Reporting of Interruptible Demands and Direct Control Load Management," which requires reporting of a forecast of interruptible demand and direct control load management data. This reporting is administrative in nature, and the information is not important for reliability. The data is best gathered through DADS and not through a standard. MOD-028-1 (all requirements); MOD-029-1a (all requirements); MOD-030-2 (all requirements) Criteria B 6 and 9 Statement: Do the ATC / TTC standards belong in NERC or NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? I think NERC should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., and I think these can/should be moved to the NAESB standards. PRC-011-0 R1 Criteria B 4 and 9 Statement: Requirements for maintenance of under-frequency load shedding systems ("UFLS") and under-voltage load shedding systems ("UVLS") are not needed to meet an adequate level of BES reliability. UFLS and UVLS installations are widely distributed. Distribution circuit outages, distribution field switching, and varying load profiles, such as peak and off-peak, could impact the amount of load that would be automatically shed by UFLS and UVLS. Therefore, entities must include adequate margins above their obligation to be able to meet the obligated load shed at all times as required by Reliability Standards, such as PRC-006 and PRC-007, that are performance-based, or results-based. While UFLS and UVLS are, of course, important safety-net systems, PRC-011-0 R 1 maintenance requirement is not needed to provide a "defense-in-depth" approach due to the margins required to meet performance-based requirements. Thus, Like PRC-008-0 R1 included in Phase I, Reliability Standard PRC-011-0 R1 which involves maintenance of UVLS, is not needed. In fact, it is typically the same relays and associated equipment that provides both the UFLS and the UVLS functions. PRC-022-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.5 Criteria B 7 Statement: Whether the responsible entity has robust UVLS misoperation and correction action is redundant with PRC-004-1a, -2a. TOP-001-1a R7 (and its subrequirements) Criteria B 9 Statement: For R3, there are three projects in progress addressing the issuance of directives by the RC, BA, and TOP. This includes COM-003-1's requirements for the issuances of "not quite directives" Also, for R7 All outages information should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-002-2b R8 and R 9 Criteria B 6, 7 and 9 Statement: "Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency", is duplicative of VAR-001 (and incorrect) and should be eliminated. "Each Balancing Authority shall plan to meet Interchange Schedules and ramps", is duplicative of the BAL standards and the NAESB standards and should be eliminated. TOP-002-2b R12 Criteria B 6 and 9 Statement: The ATC / TTC standards may belong in NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? NERC standards should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc. TOP-002-2b R14 and R14.1 Criteria B 9 Statement: All derating information should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-002-2b R15 Criteria B 9 Statement: Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations is a "how" requirement that is needed to meet other requirements in the standard. It is also not measureable, and the requirement should be eliminated. All weekly forecasts should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-003-1 R1 and its subrequirements; R2 and R3 Criteria B 9 Statement: All planned outage information should be submitted to the TOP and/or BA in accordance with their data requirements. TOP-005-2a R3 Criteria B 9 Statement: PSEs are not best positioned to provide reliability information.

The Trade Associations believe that the P81 project should be considered a high priority Standards development project for the following reasons: • Responsive to P81 of FERC's March 15, 2012 order and SPIG Recommendation No. 4 • Will increase efficiency of the ERO compliance programs • Requirements submitted for the initial phase appear to be clear candidates on their face and should not require extensive technical research • The collaborative nature of the project is an example for future work, because it advances the project while reducing the impact on stakeholders and NERC staff • The proposed pace of the project sets an example for future work • Furthers the focus on results, performance based Reliability Standards • May provide a roadmap of what should or should

not be a requirement in future Reliability Standards • The draft P81 SAR criteria are designed to be sufficiently broad to capture all FERC approved reliability Standards that are unnecessary, redundant or do little to protect reliability • Eliminating Reliability Standards requirements that are unnecessary, redundant or do little to protect reliability will eliminate distractions from our focus on reliability Based on these benefits, the Trade Associations strongly support the Standards Drafting Team and NERC staff working together to file the initial list of Reliability Standards for retirement with the Federal Energy Regulatory Commission prior to the end of the year, and that the Standards Drafting Team also make significant progress on the scope of the phase two P81 Reliability Standards list by the end of the year.

Individual

Kirit Shah

Ameren

Yes

Yes

We appreciate the excellent work done by the P81 Project team in developing the criteria and agree with the list of suggested standards/requirements that easily satisfy the criteria in this initial phase.

We support and agree with Trade Association's comments and their suggested list of Reliability Standard requirements to be retired or modified in the subsequent phase of the P81 Project. In addition, we suggest that IRO-005-3, R10 should be modify to eliminate its applicability to LSE and PSE in addition to GOP. While the IRO-005-3_1a, R10 is necessary for the reliable operation of the BES, its applicability to LSE and PSE also is questionable as these entities do not "operate" the BES. We believe that it is redundant (criteria B7) with other requirements where these entities (GOP, LSE, and PSE) have to follow the RC and/or TOP directives.

Individual

Jason Snodgrass

Georgia Transmission Corporation

Yes

Georgia Transmission Corporation agrees with the criteria listed in the SAR to identify Reliability Standard requirements for either modification or withdrawal.

No

GTC agrees that the suggested list easily satisfies the criteria in the draft SAR, but GTC also believes this is an incomplete list for Phase I. GTC also believes the following Reliability Standard requirements easily satisfy the criteria listed in the draft SAR and recommends reconsidering and adding to the list in the initial Phase I. MOD-016-1.1;R1:The Planning Authority and Regional Reliability Organization shall have documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses. [Meets Criteria A, B1, B2, B3, B9] MOD-016-1.1 R1.1 The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values. Meets Criteria A, B1, B3, B4, B9 MOD-016-1.1 R3 The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area. Meets Criteria A, B1, B3, B9 MOD-016-1.1 R3.1 The Planning Authority shall make this distribution within 30 calendar days of approval. Meets Criteria A, B1, B3, B9 MOD-017-0.1 R1 The Load-Serving Entity, Planning Authority and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R1. Meets Criteria A, B1, B4, B9 MOD-017-0.1 R1.1 Integrated hourly demands in megawatts (MW) for the prior year. Meets Criteria A, B1, B4, B9 MOD-017-0.1 R1.2 Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the

prior year. Meets Criteria A, B1, B4, B9 MOD-017-0.1 R1.3 Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years. Meets Criteria A, B1, B4, B9 MOD-017-0.1 R1.4 Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested. Meets Criteria A, B1, B4, B9 MOD-018-0 R1 The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or dispersed basis) shall: Meets Criteria A, B1, B3, B9 MOD-018-0 R1.1 Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and Meets Criteria A, B1, B3, B9 MOD-018-0 R1.2 Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load. Meets Criteria A, B1, B3, B9 MOD-018-0 R1.3 Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1. Meets Criteria A, B1, B3, B9 MOD-018-0 R2. The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days). Meets Criteria A, B1, B4, B9 MOD-019-0.1 R1. The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-1_R 1. Meets Criteria A, B1, B4, B9 MOD-020-0 R1. The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days. Meets Criteria A, B1, B4, B9 MOD-021-1 R1. The Load-Serving Entity, Transmission Planner and Resource Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed. Meets Criteria A, B1, B3, B9 MOD-021-1 R2. The Load-Serving Entity, Transmission Planner and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R1. Meets Criteria A, B1, B3, B9 MOD-021-1 R3. The Load-Serving Entity, Transmission Planner and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B9 PRC-005-1b R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include: Meets Criteria A, B1, B3, B9 PRC-005-1b R2.1. Evidence Protection System devices were maintained and tested within the defined intervals. Meets Criteria A, B1, B3, B9 PRC-005-1b R2.2. Date each Protection System device was last tested/maintained. Meets Criteria A, B1, B3, B9 PRC-006-1 R7. Each Planning Coordinator shall provide its UFLS database containing data necessary to model its UFLS program to other Planning Coordinators within its Interconnection within 30 calendar days of a request. Meets Criteria A, B1, B4, B9 PRC-006-1 R8. Each UFLS entity shall provide data to its Planning Coordinator(s) according to the format and schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. Meets Criteria A, B1, B4, B9 PRC-006-1 R14. Each Planning Coordinator shall respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the following: 14.1. UFLS program, including a schedule for implementation 14.2. UFLS design assessment 14.3. Format and schedule of UFLS data submittal Meets Criteria A, B1, B3, B9 PRC-007-0 R2. The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLSprogram database. Meets Criteria A, B1, B4, B9 PRC-007-0 R3. The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional

Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days). Meets Criteria A, B1, B3, B4, B9 PRC-011-0 R2. The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B4, B9 PRC-015-0 R3. The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days). Meets Criteria A, B1, B4, B9 PRC-017-0 R2. The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B4, B9 PRC-018-1 R5. The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years. Meets Criteria A, B1, B2, B3, B9 PRC-021-1 R2. Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request. Meets Criteria A, B1, B4, B9 PRC-023-1 R3.3. The Planning Coordinator shall provide a list of facilities to its Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within 30 days of the establishment of the initial list and within 30 days of any changes to the list. Meets Criteria A, B1, B4, B9 TOP-001-1a R4. Each Distribution Provider and Load-Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions. Same requirement as R3 which made the Phase I list, only difference is applicability.
FAC-001-0 (all requirements) Criteria B 1, 3 and 6 Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria Meets Criteria A and a combination of either or all of B1, B2, B3, B4, B 9 Statement: MOD-016 through MOD-021 are about long term load forecasting and reporting of actual and forecast loads. Requirements could be eliminated from the standards and replaced with a data collection process (e.g., TADS/DADS, etc.). Loads to be used in modeling could be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard. Additionally, MODs-016 through 021 have yet to be classified as Tier 1, 2, or 3; nor have they yet to be identified on NERC's Actively Monitored List. PRC-006-1 (R7, R8, and R14) Criteria: Meets Criteria A and a combination of either or all of B1, B3, B4, B9 Statement: Recommend these requirements to be eliminated from the standards and replaced with a data collection and or reporting process (e.g., TADS/DADS, etc.). PRC-023-1 (R3.3) Criteria: Meets Criteria A and a combination of either or all of B1, B4, B9 Statement: Recommend these requirements to be eliminated from the standards and replaced with a data reporting process. TOP-001-1a (R4) Criteria: Meets Criteria A and B1 Statement: Same requirement as TOP-001-1a (R3) which made the Phase I list, only difference is applicability.
Reliability Standard requirements are those that provide for Reliable Operation, including without limiting the foregoing, requirements for the operation of existing Facilities, including cyber security protection, and including the design of planned additions or modifications to such Facilities to the extent necessary for Reliable Operation. NERC administers other programs, such as industry alerts, reliability assessments, event and trend analyses, education, and monitoring and enforcing Reliability Standards. These other programs are designed to work in concert with Reliability Standards to support reliable operation. NERC requirements relating to administering these other programs are very important but are not Reliability Standard requirements. One of the criteria for evaluating the elimination of a Reliability Standard requirement is that it is purely reporting. There are a number of NERC requirements for these other NERC programs embedded in Reliability Standards. Most of them are purely reporting. However, to the extent that there may be other requirements for these NERC programs embedded that are not purely reporting, they should also be considered for elimination. Reliability Standards by definition are not mechanisms for the administration of those other NERC programs. GTC recommends identifying these requirements (ex. MOD-016 through 021) and

appending them to the Phase I list.
Group
SRC
Al DiCaprio
PJM
Yes
The criteria listed in the SAR capture the right categories; however, consider restructuring B1. B2 through B5 are examples of administrative requirements and should possibly be sub-items of B1. While we generally support this proposed effort and agrees with most of the criteria, the exception is B5: “The Reliability Standard requirement requires responsible entities to periodically update (e.g., annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.” Take for example the system restoration plan. An annual review is necessary to ensure that the plan recognizes BES facility changes that occurred since the last review/update. Another example is the exceptions to the cyber security policy that needs to be reviewed and approved by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Applying this criterion in a broad brush manner without looking at each requirement may result in removing requirements that are still needed for reliability. In addition, the acid test for retirement of a requirement is when the standard drafting team reviews the overall reliability impact of removing a particular requirement from a standard, and how it may affect other related standards. In brief, it may be a bit premature to pass on this judgment at the SAR stage. We urge the SAR proponent to simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired. And, in order to meet the requirements for regulatory approval, we suggest the SDT to provide strong technical basis to justify each retirement.
Yes
• PRC-009-0 R1 – R2 are in the process of being retired by PRC-006-1 as such these requirements will eventually go away. • VAR-002-WECC-1 R2 - Regional standards/requirements for retirement should go through the regional standards process not the NERC continent wide process. • VAR-501-WECC-1 R2 - Regional standards/requirements for retirement should go through the regional standards process not the NERC continent wide process. • Consider adding IRO-014-2 R2 requirements: R2 Each Reliability Coordinator shall maintain its Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 as follows: [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning] 2.1. Review and update annually with no more that 15 months between reviews. 2.2. Obtain written agreement from all of the Reliability Coordinators required to take the indicated action(s) for each update. These meet criteria B1 and B5.
Consider including the following standards for review in Phase II: BAL-004-0 – Time Error Correction MOD-030-2 – Flowgate Methodology PRC-006-1 R8 (provision of data) PRC-006-1 R14 (administrative – response to written comments)
We support the P81 team’s efforts and appreciate the effort to pull together this initial list of criteria and requirements. The SRC is looking forward to seeing a concrete timeline for the project.
Group
PPL Corporation NERC Registered Affiliates
Stephen J. Berger
PPL Generation, LLC on behalf of its Supply NERC Registered Entities
Yes
Yes
The PPL Companies generally support the concept and process being recommended, but are concerned that the stakeholder involvement in the process may be lacking. During the webinar on August 21, 2012 the drafting team members stated that the Standards Development Process will be utilized for all Phases of the project. However, the SAR does not indicate that the SDP is mandated. The Companies recommend that the entire SAR specifically state the the Standards Development

Process will be used where the SDT must respond to comments and a stakeholder vote for approval. Additionally, the process should allow for individual (or groups) of stakeholders to request a standard's removal or modification that is not designated by the SDT for removal.
Group
Western Electricity Coordinating Council
Steve Rueckert
WECC
No
WECC offers the following related to the criteria listed in the SAR. WECC beleives the OVERARCHING CRITERIA listed under "A" needs clarification and that as currently identified is too vague. The Overarching Criterion statement is too broad and is contrary to the FPA Section 215. "Impact" is an ambiguous term. There is no measure as to how to quantify a Requirement's "impact" and to distinguish between "little" impacts as opposed to some other metric of "impact." More importantly, however, a Requirement that has any impact on the reliable operation of the BES cannot be dismissed as inconsequential, even if it is determined to have "little" impact. The "impact" must be weighed against the "burden" of the standard and potential for efforts to demonstrate compliance hindering or preventing other more "impactful" reqiurements. Further, the Standard Requirements work in concert with one another. For many Standard Requirements, it is impossible to reasonably assess the "impact" of a single Standard Requirement. For example, the "purpose" statement for CIP Standard Requirements reads that "[CIP Standard Requirements] should be read as part of a group of standards numbered Standards CIP-002 through CIP-009." To examine the "impact" of a single Standard Requirement, therefore, contradicts the intent and purpose of many Standard Requirements that are crafted to operate in concerns with one another. WECC believes the B1 Administrative Technical Criteria needs claificaiton and is vague as currently written. The term "administrative" is ambiguous and could cover a broad range of activities. Further, "administrative requirements" often require evidence of program or procedure creation. However, WECC does agree with this criteria, but only in the case where all three criteria listed (administrative, does not support reliability, and needlessly burdensome) are met. WECC disagrees witht he B2 Technical Criteria Data Collection/Data Retention. Data Collection/Data Retention is often the only means by which a Responsible Entity can objectively demonstrate compliance. As to mandatory data retention periods, an explicit mandate to retain data may be required to meet compliance obligations unique to a particular Standard Requirement. However, if treated correctly, a requirement for the data collection/retention for compliance purposes could be removed from the Requirmeetns and made part of the Measures or RSAWs. WECC Disagrees with the B3 criteria Purley Documentation unless it can be clearly demonstrated that the dcoumentation does not protect the reliabiltity of the BES in any way. In some cases Plans/Policies/Procedures are necessary for employees to have a guide for not only protection but maintaining and restoring BES assets (i.e. Restoration Plans). Documentation of plans, policies and procedures, is key in defining the parameters of compliance. Further, plans/policies and procedures are often the only means by which Compliance and Enforcement can assess a responsible entity's compliance with a Standard Requirement. WECC Disagrees with the B4 criteria Purely Reporting unless no purpose for the reporting can be identified. Reporting helps overarching organizations (ex. ES ISAC) detect potential issues earlier, by giving them more information and from multiple entities. These issues may seem small or insignificant when viewed by a singular entity but may have a more a drastic impact when viewed from the perspective of the entire BES. WECC Disagrees with the B5 criteria Periodic Updates unless it can be clearly demonstrated that the reproting has no operational benefit to reliability. Without these requirements there is nothing in place to ensure entityies are maintaining, and periodically verifying the accuracy of these documents. With the criteria established as it is, there is no real way of measuring the effect of "operational benefit to reliability". Is it measured by the size of impact (MW), by time (something that will take over a 1hr), or by Time Horizon (Same-Day operations vs. Real Time Operations). It is recommended to establish a more accurate means to measure these criteria. If proberly handled, these reporting requirements that that demonstrate the entities are maintaining certain necessary documents could be moved from the Requirements to the Measures or RSAWs. WECC agrees with the B6 criteria of Business Practices. B7 criteria Redundant: Although WECC agrees requirements should not be redundant with each other, if compliance is left to other regulators (Open Access Transmission Tariff, NAESB, etc.) compliance may not be held up to NERC expectations or interpretations. In identifying redundant standards, only NERC Reliability Standards should be considered. WECC agrees with B* criteria, WECC believes the B9

criteria needs clarification and as written is vague. How will the determination that teh Requirements do little, if anything, to promote the protection of the BES be determined? WECC disagrees with C1. The FFT determination is not predicated on any particular Standard Requirement. The FFT determination is fact specific. Even a requirement that is critical to the BES may have an FFT'd violation if the manner in which the requirement was violated was minor. WECC beleives C2 is vague and needs clarification. Not certan what it means if the requirement is being revieweed in an on-going Standards Development Project. Is this the same as B7 Redundant? WECC agrees C3 is a factor that should be considered. WECC agrees with C4 but beleives information on how the tiers will be viewed should be included. WECC agrees with C5. WECC believes C6 and C7 are vague as written and believes that these last two reference points are intended to indicate that if the answer is yes, then the requirement or standard would NOT be eligable for retirement. This should be clarified.

No

WECC supports the majority of the Standards Requirements identified, but notes concerns with the following. WECC recommends eliminating CIP-003 R1 in its entirety. WECC disagrees with the inclustion of CIP-007, R7.3. This requirement is necessary for entity's to demonstrate compliance with the other sub-requirements of CIP 007 R7. However, this requirement could be moved to a Measure or RSAW to demonstrate compliance with the other sub-requirements of CIP-007, R7. WECC disagrees with the includsion of IRO-016-1, R2. Required documentation of the RC's actions to remedy an event is necessary for quality and efficient root cause analysis, including insight into the RC's wide view of actions during an event or disagreement. The language in the SAR statement for IRO-016-1 R2 points to this information being monitored through Spot Checks or other compliance monitoring methods. If this standard is removed yet the information is to be included in future compliance monitoring there must be some sort of methodology that requires the entity to retain the associated data to be kept for the duration of the required cycle for monitoring (i.e. audit cycle if monitored through audits). It is important that entities document the actions taken that analyze the effect on the system as well as the BES for either an even or/and for the disagreement on the problem. Therefore, it is important that this information is part of the overall compliance monitoring program. MOD-004 is not redundant to TOP-002 even though the CBM itself may be a tariff issue and rarely used. The reliability piece is that if the CBM is used by a TSP then the details of it must be available for use in system studies. Without the awareness of a transmission holdback for CBM when it exists, a network study could be run and show no issues but if at some time the CBM were implemented an overload could result. This might not always be the case but unless the CBM parameters are known and modeled it could impact reliability. WECC disagrees with the recommendations with PRC-008-0 R1 and PRC-008-0 R2. Unless these standards are being superseded, WECC does not agree that they provide "little protection to the BES." They are not administrative in nature like the other standards in this group. They insure that maintenance and testing program is established and implemented for an entity's UFLS protection systems. Without these standards, there is reduced assurance that UFLS protection systems will operate correctly when called upon for an under-frequency event. UFLS has a vital role in its effectiveness for preserving system stability and elimination of these standards may reduce its effectiveness. This standard is about making sure the equipment is maintained not about collecting data. If and when PRC-005-2 is adopted, and if it were to include the UFLS devices, then this standard should be considered for removal. WECC believes the statements associated with TOP-001-1a, R3 are incorrect. Removing TOP-001-1a would result in no NERC requirement for parties to follow TOP directives. The current TOP-001-1a R3 requires BOTH TOP and RC directives to be followed. The proposed IRO-001-3 R2 requires ONLY RC directives to be followed. In addition, the SAR statement is incorrect. TOP-001-1a R3 applies to directives issued by the TOP (and also the RC). IRO-001-1a applies only to directives from the RC. If the intent, as they state, is to replace TOP-001-1a R3 with IRO-001-3, that leaves a void for an entity to comply with a directive from the TOP. Only the part about following an RC directive is redundant. Requirement should be modified to eliminate the redundancy, but not retired. WECC disagrees witht he inclusion of CIP-001, R4. An entity has many enforcement agencies to contact without the FBI listed in the operating instructions they could easily be overlooked. This Requirement has encouraged entities to establish a current communication line with the FBI. In fact, several other larger entities are members of InfraGard®, which is a partnership between the FBI and the private sector. Retiring R4 will remove the incentive of having a working relationship with the FBI, especially among the smaller entities. Retiring R4 may effectively delay or prevent the FBI from rapidly locating those responsible for sabotage. The requirement is not "needlessly burdensome", which is a criteria for deletion. WECC believes the requirements VAR-002-WECC-1, R2, and VAR-502-

WECC-1, R2, are probably the best way of demonstrating compliance with the accociated R1 requirments. The two VAR R2 requirements do not say the entity has to submit the information to WECC (Regional Entity), only that it shall have the documentation to prove exclusion for the sub requirements in R1. We've had cases where entities don't meet the 98% availability and if the entity was claiming exclusion time, WECC would want to review the documentation that proves the exclusion. It is in the entity's best interest to keep exclusion documentation in case its units don't make the 98%, but this is beter suited for a Measure or RSAW.
CIP 002 R2/R3/R4: Redundant and require revision. Each of these requirements requires an annual review of the Critical Asset list and Critical Cyber Asset list. WECC agrees these protections are required, however, the standard should be revised so either CIP 002-3 R4 is removed and CIP 002-3 R1-R3 are revised to require annual review and approval of the appropriate documentation, or CIP 002-3 R2 and R3 are revised to no longer require an annual review. CIP 005 R1.5/006 R3: These are redundant and should be removed/revised. CIP 006-3 R3 is redundant with CIP 005-3 R1.5. Either CIP 005-3 R1.5 should be revised to no longer require the protections of CIP 006-3 R3, or CIP 006-3 R3 should be removed and the content of CIP 006 R3 moved to CIP 005 R1.5. CIP 005 R1.5/006 R2.2: Redundant. Should be revised. Devices applicable to these requirements may be redundant if they are classified as CCA (thus duplicated with CIP 002 – CIP 009) or reside within an ESP (thus duplicated with CIP 007). The requirements should be revised to take into account the situation where a device resides within an ESP or is classified as CCA, and is a device used in the EACM/PACM of ESPs/PSPs. Note: It appears this is being addressed in V.5 of CIP. CIP-005, R5: Should be removed and the protections highlighted in this requirement moved to appropriate requirements it references. This will cause less confusion with entities, and be more precise with exactly what documentation is required to be reviewed and approved. CIP 005 R5.1/R5.2: Redundant. Should revise CIP 005 R1.6 to include the wording of CIP 005 R5.1, and remove CIP 005 R5.1. This will cause less confusion with entities, and be better aligned with the CIP 005 R1.6 requirement. CIP 005 R5.3: Redundant. Should revise CIP 005 R3 to include the wording of this sub-requirement, and CIP 005 R5.3 should be removed. This change will create a better fit in the appropriate requirement, and be less confusing for entities. CIP 007 R9: Should be removed and the protections highlighted in this requirement moved to appropriate requirements it references. Thus CIP 007 requirements that require documentation should include the need to review and update the documentation. This will cause less confusion with entities, and be more precise with what documentation is required to be reviewed and approved. EOP-004-1 R3.2: Little, if any, value as a reliability requirement. This requirement points to attachments that could be addressed in the main part of the R3 standard. This requirement does nothing to promote the protection of the BES. VAR-001-2 R10: Redundant. The reliability purpose for R10 is to make sure that operators don't think that exceeding an SOL or IROL due to voltage issues is acceptable. There are multiple standards requiring operators not exceed and maintain an SOL or IROL with 30 minutes, regardless of the cause of the exceedance. These standards are TOP-001-2 R7, R11; TOP-004-2 R1; TOP-007-0 R2; TOP-008-1 R1.
WECC recognizes and appreciates the large amount of work done in a short time on this project and appreciates the opportunity to proved our comments.
Group
Tampa Electric Company
Ron Donahey
Tampa Electric Company
Yes
Yes
Tampa Electric suggests that the P81 Drafting Team consider the adoption of concepts from the CIP version 5 criteria for consideration under CIP version 3 and 4. In particular Tampa Electric proposes that draft language for CIP-007 patching will reduce administrative burden for compliance with patching process TFEs under current versions (CIP-007 V3 and V4). The version 5 draft Guidelines and Technical Basis for CIP-007 V5 states: R2.1 A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. R2.2 Determination that a security related

patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.
Tampa Electric recommends that the P81 DT ensure that the CIP requirements proposed for removal via P81 are also removed from v5 of the NERC CIP standards. Tampa Electric also supports the consideration of the following for NERC CIP standards: Removal of data collection requirements: CIP-005-3a, -4a R5.3 CIP-006c, -4c R7, R8.3 CIP-007-3, -4 R5.1.2; R6.4; R7.3 CIP-008-3, -4 R2 Removal of annual review requirements: CIP-002-2, -4 R4 CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3 CIP-006-3c, -4 R1.8 CIP-007-3, -4 R9 CIP-009-3, -4 R1
Individual
Kristin Iwanechko
NERC
No
(1) Revise Criteria A to focus on the content of the Reliability Standards. NERC Staff suggests the following language for Criteria A: “The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to protect reliable operation of the BES.” This language is currently included as Criteria B9. NERC notes that both Criterion B8 (hinders the protection or reliable operation of the BES) and B9 (little, if any value as a reliability requirement) are duplicative with Criterion A and should be eliminated. Since any requirement that meets Criterion B8 or B9 would necessarily meet Criterion A, this creates an unintended consequence by undermining the objective that requirements for consideration must satisfy both the overarching Criterion A and a separate technical criteria. For these reasons, NERC Staff supports the elimination of both Criteria B8 and B9 and the re-phrasing of Criteria A. (2) There is significant overlap between Criteria B3 (Purely Documentation) and B5 (Periodic Updates) and these criteria could be combined. Criteria B3 addresses requirements for entities to develop a document that is not necessary and Criteria B5 addresses the requirement for entities to periodically update such documentation. NERC Staff suggests renaming Criteria B3 “Documentation” and suggests the following language: “The Reliability Standard requirement requires responsible entities to develop and/or periodically update a document (e.g., plan, policy or procedure) which is not necessary to protect BES reliability.” (3) The explanation of Criterion B6 (Commercial or Business Practice) states that the Reliability Standard requirement “is a commercial or business practice, e.g., better served as a NAESB standard or as part of NAESB Electric Industry Registry (EIR).” However, the technical justifications provided for the application of the B6 criteria do not state that the standard/requirement should be addressed in another manner, e.g., with a NAESB standard. Please clarify or otherwise modify this criterion appropriately. Further, the technical justification should address the fact that such business practices may not be applicable to the same entities and may not be mandatory or enforceable.
No
After further review, NERC Staff recommends that the SDT review the following standard requirements and consider moving them from Phase I to Phase II. If the SDT determines the following standard requirements still fall into Phase I, a more robust technical justification would be needed. (1) FAC-008-1 R2, R3, FAC-008-3 R4, R5 and FAC-013-2 R3: These requirements, combined with others, provide checks and balances on the Facility Rating Methodology and Transfer Capability methodology established by the responsible entities. This provides a reliability benefit by requiring the responsible entity to consider areas in which their methodology may not be sufficient to support reliable operation of the interconnected transmission system. There may be better ways of assuring that entities have sufficient methodologies and alternatives should be considered during Phase II. NERC Staff suggests that the SDT reconsider whether discussing the methodology (and not the numerical rating of a facility) has commercial or market related implications. With respect to FAC-013-2 R3, NERC Staff suggests that the SDT reconsider whether the requirement relates to “a back and forward on transfer capability” as noted in the draft SAR, as the requirement pertains only to the methodology for determining transfer capability. (2) PRC-008-0 R2: Maintenance and testing of underfrequency load shedding (UFLS) relays is necessary to assure reliable operation of a UFLS program and this requirement is included in PRC-005-2 as part of Project 2007-17, Protection System Maintenance and Testing. NERC Staff recommends that the language in R2 relating to implementing its UFLS equipment maintenance and testing program remain to avoid a reliability gap prior to the effective date of PRC-005-2. NERC Staff recognizes that the second part of R2 does meet the criteria in the SAR and recommends that the SDT consider revising the requirement in a future phase to

remove the language that requires an entity to “provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).” (3) TOP-001-1a R3: The technical justification states that this requirement is redundant with IRO-001-1a R8. NERC Staff notes that the requirement is only partially redundant until IRO-001-3 is approved by FERC and therefore, it is premature to consider it for Phase I; it should be considered for Phase II. (4) MOD-004-1: NERC Staff notes that there are a number of Commission directives associated with MOD-004-1 and the technical justification provided for the elimination of this standard should directly address these directives. If a solid technical justification cannot be made, NERC Staff suggests that the requirements should not be included in Phase I. In addition to the above, NERC Staff recommends that the SDT consider removing the following standard requirements from the scope of the P81 project: (1) PRC-008-0 R1: The requirement to have a maintenance and testing program for UFLS is necessary to assure reliable operation of a UFLS program and this requirement is included in PRC-005-2 as part of Project 2007-17, Protection System Maintenance and Testing. NERC Staff recommends retaining R1 to avoid a reliability gap prior to the effective date of PRC-005-2. (2) PRC-009-0 R1: Analysis to assess the performance of UFLS equipment and program effectiveness following system events provides a reliability benefit by identifying whether the UFLS program is effective and whether modifications are necessary. A requirement similar to R1 is included in FERC-approved standard PRC-006-1 and NERC Staff recommends retaining R1 to avoid a reliability gap prior to the effective date of PRC-006-1. If the SDT believes this requirement is not necessary, the justification for removing R1 should discuss Commission comments in Order No. 763 pertaining to Requirement R11 in PRC-006-1. (3) VAR-002-WECC-1 and VAR-501-WECC-1: NERC Staff notes that the regional standards should be removed from the scope of the P81 project because they must first be eliminated via the regional standards development process prior to being processed through the NERC standard development process.
Please see NERC Staff’s response to question 2 for Phase I requirements that NERC Staff recommends be reviewed for inclusion in a future phase. NERC Staff may propose additional requirements for a future phase of the P81 project at a later date.
(1) NERC Staff notes that the scope of the SAR should be expanded to include currently-pending versions of related Reliability Standards to address requirements proposed in Phase I that are also included in a subsequent version of the standard that has been adopted by the NERC Board of Trustees, but not yet approved by FERC. NERC Staff suggests that footnotes could be included to capture these situations. (2) NERC Staff submits that the technical justification for removal of particular requirements should not be a restatement of the Criteria (see e.g., INT-007-1 R1.2). Nor should the technical justifications reference and/or rely upon for support any Reliability Standards unless those Reliability Standards are Commission-approved. (3) NERC Staff suggests that the technical justifications for the satisfaction of the Criteria should include an explanation of how removal of the requirement will result in an “increase in efficiency of the ERO compliance program” consistent with the language of P81.
Individual
Cheryl Moseley
Electric Reliability Council of Texas, Inc.
Yes
ERCOT agrees with the ISO/RTO SRC comments. However, in addition for SRC comments, ERCOT offers the following: ERCOT agrees with the criteria listed in the SAR to identify Reliability Standard requirements for retirement in Phase 1. However, the criteria used for future phases should remain flexible. The initial list should not preclude the use of additional criteria for future phases where additional criteria support the elimination of requirements in those efforts.
Yes
ERCOT agrees with the ISO/RTO SCR comments. However, in addition to the SRC comments, ERCOT offers the following: ERCOT agrees that all the requirements included in the SAR warrant retirement based on the relevant criteria, as supported by the corresponding justification statements. ERCOT offers the following additional comments related to the justification statements for the SDT’s consideration: BAL-005-0.1b R2 – The justification statement could benefit from additional clarification regarding the reason why this requirement is redundant, because it isn’t readily apparent why this is redundant with BAL-001 R1 and R2. Maintaining CPS requires the use of regulation. Therefore, it is implicit that the relevant functional entities have regulation to comply with BAL-001 R1

and 2. Also, the justification should clarify the point of the discussion related to equating compliance based on compliance of BAL-001 R 1 and 2 and how that argument justifies retirement. CIP-001-2a R4 – The justification statement should clarify that this requirement is redundant to the communications obligations in R1-3. CIP-003-3, 4 R1.2 – In addition to the justifications presented in the SAR, the term "readily available" is ambiguous and creates the opportunity for the use of CEA subjective judgment during compliance assessments. This is problematic for compliance risk generally, but is especially problematic when the requirement is administrative in nature. Entities should not be subject to unnecessary compliance risk based on ambiguity that can result in subjective compliance determinations based on the opinion of CEA personnel, as opposed to the four corners of the requirements, especially when the underlying requirement provides no reliability value. Further evidence that this requirement serves no purpose is the fact that it is not included in CIP v5. CIP-003-3 R3, 3.1, 3.2 and 3.3 – In addition to the justifications presented in the SAR, this issue is already fully addressed in the TFE process in Appendix 4D of the ROP, which is not only adequate, but is the appropriate place for this type of administrative function related to documentation. There are a specific set of defined requirements that allow an exception, and those exceptions have be to be filed according to the TFE process. Thus, the requirements proposed for retirement are redundant to that process. CIP-003-3, -4 R4.2 – In addition to the justification presented in the SAR, the phrase "based on sensitivity", is ambiguous and creates the opportunity to insert subjective judgment into compliance assessments. This is problematic for compliance risk generally, but especially when the requirement is administrative in nature AND redundant. Entities should not be subject to unnecessary compliance risk based on ambiguity resulting in subjective compliance determinations, as opposed to the four corners of the requirements, especially when the underlying requirement provides no operational reliability value. Further evidence that this requirement serves no purpose is the fact that it is not included in CIP v5. CIP-005-3a, -4a R2.6 – The justification statement could benefit from additional clarification as to why the banner is not useful. An appropriate use banner has not been useful over time, because people who intend to use sites inappropriately will simply ignore the banner. Banners are generally considered to be a legal protection and not a security protection. Further evidence that this requirement serves no purpose is the fact that it has been removed from CIP v5 because the use of banners does not meet a reliability objective. CIP-007-3, -4 R7.3 – In addition to the justification presented in the SAR, it should be noted that to demonstrate that an entity performed the data destruction under R7.1 and R7.2, the entity needs to collect evidence. Having a separate requirement for evidence is redundant and not needed. COM-001-1.1 R6 – In addition to the justification presented in the SAR, the justification statement could note that this policy should be documented in the ROP for information within NERCNet that is considered sensitive or impacting to the BES. It should be a voluntary best practice or business practice for other information so that entities may use it, or use some other policy that better fits its circumstances. The justification should state that the NERCNet policy should be a voluntary best practice type of issue for information that is not considered sensitive or impacting to the BES. EOP-009-0 R2 – This is a reporting obligation and a documentation issue. The justification statement should also note that both documentation and reporting on this does not rise to the level of a reliability standard. The statement could note that this may be a best practices issue, but just for documentation. Reporting test results to REs isn't a best practice. Additionally, the justification should not state that the relevant information is better considered / obtained during an audit. If it's not relevant to the mandatory requirements, then it has no place in CMEP proceedings. FAC-002-1 R2 - The justification should not include that the relevant information is better considered / obtained during an audit. If it's not relevant to the mandatory requirements, then it has no place in CMEP proceedings. FAC-008-1 R1.3.5 – In addition to the justification presented in the SAR, the justification statement could note that the term "other assumptions" is ambiguous and introduces the potential for inefficient/ineffective administration of the CMEP due to introduction of subjectivity and opinions into compliance assessments. This is problematic for compliance risk generally, but especially when the requirement is administrative in nature AND redundant. Entities should not be subject to unnecessary compliance risk based on ambiguity resulting in subjective compliance determinations, as opposed to the four corners of the requirements, especially when the underlying requirement provides no operational reliability value. FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5 – In addition to the justification presented in the SAR, the justification statement could note that it is inappropriate for entities other than the owners of equipment to establish facility ratings. The owners don't have to change their ratings, but the scheme is far more effective if the respective functional roles are distinct and not blurred by the review process contemplated in the requirements proposed for retirement. The

owners should set the ratings and the RCs receive them and perform their functions in accordance with those ratings. The RC should not be involved with the TO/GO business-management of their equipment. Also, by keeping the roles distinct, it mitigates any liability risk of the third party if the owner uses its input and then the equipment breaks because of the new rating; FAC-013-2 R3 – Same comment as above. MOD-004-1 R1; MOD-004-1 R1.1; MOD-004-1 R1.2; MOD-004-1 R1.3; MOD-004-1 R2; MOD-004-1 R3; MOD-004-1 R3.1; MOD-004-1 R3.2; MOD-004-1 R4; MOD-004-1 R4.1; MOD-004-1 R4.2; MOD-004-1 R5; MOD-004-1 R5.1; MOD-004-1 R5.2; MOD-004-1 R6; MOD-004-1 R6.1; MOD-004-1 R6.2; MOD-004-1 R7; MOD-004-1 R8; MOD-004-1 R9; MOD-004-1 R9.1; MOD-004-1 R9.2; MOD-004-1 R10; MOD-004-1 R11; MOD-004-1 R12; MOD-004-1 R12.1; MOD-004-1 R12.2; MOD-004-1 R12.3 – ERCOT agrees with the comments/justifications. PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 – In addition to the justification presented in the SAR, the justification statement could note that the tasks required in these standards are administrative/documentation/reporting in nature and they don't affect reliability from a standards perspective. These could either be best practices or evidentiary in RSAWs – e.g. provide UFLS/UVLS program documentation – which could be relative to requirements that have actionable UVLS/UFLS requirements; TOP-001-1a R3 – ERCOT agrees with the justification with regard to the RC function, but the TOP standard also requires BAs/GOPs to follow the directives of the TOP, so the two relevant requirements are not apples to apples. Modification to one or the other may be needed to ensure appropriate authority and corresponding obligation to follow that authority is reflected in one or the other standard, or both, but eliminate overlaps. TOP-005-2a R1 – ERCOT agrees with the justification. This should either be in the ROP or just via the ISN access process/agreement. VAR-002-WECC-1 R2; VAR-501-WECC-1 R2 – ERCOT agrees with the justification, but if the documentation/reporting are not relevant for the requirement, then the SAR should not suggest the REs should seek the info in CMEP proceedings, which should solely focus on compliance with the substance of the standards.
ERCOT agrees with the ISO/RTO SCR comments. However, in addition to the SRC comments, ERCOT offers the following: ERCOT supports future phases of the P81 project to eliminate/retire reliability standards that do not facilitate BES reliability. ERCOT is reviewing all standards to that end, however, developing a list of additional requirements for retirement will require additional time. The SDT should establish a prospective process that provides adequate time and opportunity for entities to perform a meaningful review of remaining requirements to determine which additional requirements warrant retirement and to develop appropriate criteria, if relevant, that may be incremental to the ones proposed in this SAR, and to develop appropriate retirement justifications based on the relevant retirement criteria.
This SAR offers significant potential value by retiring requirements that provide no BES reliability value, but nonetheless require commitment of time and resources for both regulated entities and regulators to effect and oversee compliance, respectively, and also pose liability risk for no reason, given that they provide no reliability value. However, the substance of the requirements (e.g. administrative processes, etc.) may have non-essential value unrelated to system reliability. To the extent the SDT/industry/NERC believe there may be some non-mandatory use for this information outside of the reliability standards, the information could be considered for guidance in another format, such as guidelines, best practice documentation or lessons learned. If such an effort is deemed worthwhile, it should be established in a separate process/effort, and should not distract from moving this and future phases of this SAR forward in the most efficient and effective manner to achieve the significant benefits that may result from this SAR. In addition, the standards process going forward should include consideration of whether a proposed standard addresses a reliability requirement, is cost effective and meets the reliability-based standards criteria of "what" needs to be met and not "how" an entity will meet the standard which is better address through guidelines, best practices and/or lessons learned.
Individual
Brett Holland
Kansas City Power & Light
Yes
Yes

Efforts need to be made to make sure that the retirement of the requirements listed in "Proposed Requirements for Retirement in Phase 1 of Project 2013-02: Paragraph 81" don't have a ripple impact in other standards or requirements.
Individual
Judy VanDeWoestyne
MidAmerican Energy Company
Yes
No
FERC Order 706 clearly states that an exception forms alternative obligations for the responsible entity to meet the requirements; an exception is not an exemption from the requirements. We believe a Responsible Entity should still be allowed to have exceptions to its cyber security policy. MidAmerican Energy Company agrees with the proposed removal of CIP-003-3 (CIP-003-4) R3, R3.1, R3.2, R3.3, as long as CIP-003-3 (CIP-003-4) R2.4 remains and allows for possible exceptions to a Responsible Entities' cyber security policy. R2.4 states "The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy." When removing requirements eligible for TFEs, revisions to the Rules of Procedure Appendix 4D – Procedures for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards will be necessary. For example, CIP-005-3, R2.6 should be deleted from the list of requirements with TFEs in the Scope section on page 1 if the requirement is removed as part of this process.
Consider the list provided by EEI.
MidAmerican Energy Company supports the draft SAR as a positive step to allow Responsible Entities, Regional Entities, NERC and FERC to focus their combined efforts on protecting the Bulk Electric System.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2013-02 Paragraph 81

The Paragraph 81 Drafting Team thanks all commenters who submitted comments on the Project 2013-02 Paragraph 81 - Retirement of Reliability Standard Requirements. The complete set of standards with proposed retirements for Phase 1 were posted for a 30-day public comment period from August 3, 2012 through September 4, 2012. Stakeholders were asked to provide feedback on the set of standards through a special electronic comment form. There were 43 sets of comments, including comments from approximately 98 different people from approximately 65 companies representing all of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Lee Pedowicz	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Ben Wu	Orange and Rockland Utilities	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Carmen Agavriloai	Independent Electricity System Operator	NPCC	2
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Michael Jones	National Grid	NPCC	1
10.	Donald Weaver	New Brunswick System Operator	NPCC	2

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Michael R. Lombardi	Northeast Utilities	NPCC	1
12.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1
16.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
18.	Brian Robinson	Utility Services	NPCC	8
19.	Michael Schiavone	National Grid	NPCC	1
20.	Wayne Sipperly	New York Power Authority	NPCC	5

2.	Group	Jim Kelley	SERC EC Planning Standards Subcommittee	X				X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Sullivan	Ameren	SERC	1
2.	Bob Jones	Southern Company Services	SERC	1
3.	Pat Huntley	SERC	SERC	10
4.	Darrin Church	TVA	SERC	1

3.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

No additional members listed.

4.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tedd	Snodgrass	WECC	1
2.	Tim	Loepker	WECC	1
3.	Erika	Doot	WECC	3, 5, 6
4.	Alfredo	Bocanegra	WECC	1

5.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Louis Slade		RFC	5, 6
2.	Mike Garton		NPCC	5, 6
3.	Randi Heise		MRO	5, 6
4.	Mike Crowley		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michelle Corley	Cleco Power	SPP	1, 3, 5
2.	Eric Ervin	Westar Energy	SPP	1, 3, 5, 6
3.	Greg Froehling	Rayburn Country Electric Cooperative	SPP	3
4.	Jonathan Hayes	Southwest Power Pool	SPP	2
5.	Louis Guidry	Cleco Power	SPP	1, 3, 5
6.	Bo Jones	Westar Energy	SPP	1, 3, 5, 6
7.	Tiffany Lake	Westar Energy	SPP	1, 3, 5, 6
8.	John Mason	City of Independence, MO	SPP	3
9.	Valerie Pinamonti	American Electric Power	SPP	1, 3, 5
10.	Patrick Smith	Westar Energy	SPP	1, 3, 5, 6
11.	Ashley Stringer	Oklahoma Municipal Power Authority	SPP	4

7.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Godfrey	Pepco Holdings Inc	RFC	1, 3

8.	Group	Jason Marshall	ACES Power Marketing Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 5
2.	Scott Brame	North Carolina Electric Membership Corporation	RFC	1, 3, 4, 5
3.	Bill Watson	Old Dominion Electric Cooperative	SERC	3, 4

9.	Group	Mark S. Gray	The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA)	X		X	X	X	X	X	X		

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			(collectively, the Trade Associations).										
www.eei.org/ for members													
10.	Group	Stephen J. Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda L. Truhe	PPL Electric Utilities Corporation	RFC	1
2.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3
3.	Annette M. Bannon	PPL Generation, LLC on behalf of its Supply NERC Registered Entities	RFC	5
4.			WECC	5
5.	Elizabeth A. Davis	PPL Energy Plus, LLC	MRO	6
6.			NPCC	6
7.			SERC	6
8.			SPP	6
9.			RFC	6
10.			WECC	6

11.	Group	Steve Rueckert	Western Electricity Coordinating Council											X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Phil O'Donnell	WECC	WECC	10
2.	Brent Castagnetto	WECC	WECC	10
3.	Tim Reynolds	WECC	WECC	10
4.	Tyson Jarrett	WECC	WECC	10

12.	Individual	Bob Steiger	Salt River Project	X		X		X	X					
13.	Individual	Al DiCaprio	SRC		X									
14.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X					
15.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X					
16.	Individual	Scott McGough	Georgia System Operations Corporation			X	X							
17.	Individual	Ronnie C. Hoeinghaus	City of Garland	X		X								
18.	Individual	Dan Miller	Entergy Services, Inc.	X		X			X					
19.	Individual	Michael Falvo	Independent Electricity System Operator		X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
20.	Individual	Michelle Clements	Wolverine Power Supply Cooperative, Inc.	X									
21.	Individual	Thomas C. Duffy	Central Husdon Gas & Electric Corporation	X		X							
22.	Individual	John Tolo	Tucson Electric Power	X									
23.	Individual	paul haase	seattle city light	X		X	X	X	X				
24.	Individual	Thad Ness	American Electric Power	X		X		X	X				
25.	Individual	John Seelke	Public Service Enterprise Group	X		X		X	X				
26.	Individual	Jose H Escamilla	CPS Energy	X		X		X					
27.	Individual	Laura Lee	Duke Energy	X		X		X	X				
28.	Individual	Rich Salgo	NV Energy	X		X		X					
29.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
30.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
31.	Individual	Michelle R. D'Antuono	Occidental Energy Ventures Corp.			X		X		X			
32.	Individual	Patrick Brown	Essential Power, LLC					X					
33.	Individual	Becky Stewart	Idaho Power Company	X		X							
34.	Individual	Kimberly Tolbert	Occidental Power Services, Inc.			X							
35.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
36.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
37.	Individual	Eric Olson	Transmission Agency of Northern California	X									
38.	Individual	Kirit Shah	Ameren	X		X		X	X				
39.	Individual	Jason Snodgrass	Georgia Transmission Corporation	X									
40.	Individual	Kristin Iwanechko	NERC Staff Technical Review										
41.	Individual	Cheryl Moseley	Electric Reliability Council of Texas, Inc.		X								
42.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				
43.	Individual	Judy VanDeWoestyne	MidAmerican Energy Company	X		X		X	X				

1. **Do you agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement? If not, please explain in the comment area.**

Summary Consideration:[2]

The majority of commenters supported the Criteria A, B and C included in the draft SAR, with a few commenters suggesting changes.

A. Comments on Criterion A

The P81 standards drafting team (P81 SDT), in conjunction with NERC's technical staff review, believes it is appropriate to rephrase Criterion A to be similar to Criterion B 9, which comports with the FFT Order, and, at the same time, to eliminate Criterion B 8 and Criterion B 9 to avoid any confusion between Criterion A and Criterion B. The P81 SDT believes the following provides a more suitable overarching Criterion A:

"The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES."

Comments

The Western Electricity Coordinating Council (WECC) and Northeast Power Coordinating Council (NPCC) requested clarification or alternative wording of Criterion A, while Independent Electricity System Operator and NPCC also saw Criterion A and Criterion B 9 as redundant or duplicative. Manitoba Hydro also believed there was a need to clarify Criterion B 9 and Occidental Energy Ventures Corp. desires that Criterion A implicate Section 215 of the Federal Power Act, while Occidental, like others, also believes Criterion B 8 and Criterion B 9 need clarification.

Response

The P81 SDT believes the above revision of Criterion A and elimination of Criterion B 8 and Criterion B 9 addresses the commenters' concerns, while still including the Section 215 term reliable operation.

B. Comments on Criterion B

[2] Although responses to informal comments are not required in the detail found in the P81 SDT responsive comments, the P81 SDT believed it was appropriate to provide more detail given the level of interest in this Standards Development Project. The format and detail of these responses are not precedent setting with respect to how other SDTs respond to an informal comment period.

Comment

WECC states it only agrees with Criterion B 1 if each administrative requirement meets all the sub-requirements listed (administrative in nature, does not support reliability and needlessly burdensome). In addition, ACES Power Marketing Standards Collaborators states that in Criterion B 1 it would be best to strike "and is needlessly burdensome."

Response

The list of requirements was meant to apply to each candidate and uses the term "and" not "or" to ensure all three are required. The wording of Criterion B 1 was carefully considered in the collaborative process, and it was believed that the current wording, which tends to match with WECC's understanding, is appropriate. Thus, the P81 SDT believes that no changes to Criterion B 1 are necessary.

Comment

WECC disagrees with Criteria B 3, B 4 and B 5 unless it may be demonstrated that there is no benefit to reliability at all.

Response

WECC's comment seems misaligned with FERC's intention which the P81 SDT believes was for NERC and stakeholders to investigate what requirements provide little protection to the BES, are unnecessary or redundant. WECC's approach seems much stricter and seems to suggest that if any plausible argument can be made, the requirement cannot be retired. Such an argument is not in line with the rest of the commenters and, therefore, will not be adopted. In addition, as the project proceeds through the standard drafting process, sufficient technical justifications will be put forward for industry review for each proposed requirement for retirement. The industry will have further opportunity to evaluate the technical justifications as the P81 project moves forward.

Comment

SRC believes that the SAR captures the right categories, but states that Criteria B 2 through B 5 could be sub-items of B1. In a similar light, NERC staff states there is significant overlap between Criterion B 3 (Purely Documentation) and Criterion B 5 (Periodic Updates) and these criteria could be combined. Independent Electricity System Operator and SRC also disagree with Criterion B 5.

Response

While annual reviews may be necessary, there may be other ways to ensure periodic reviews are done. Criterion B 5 was contemplated by the P81 SDT more in the context of future phases which would allow for the modification of requirements, not an easily identified retirement. Thus, while to some extent we share the concerns of SRC, NERC staff and Independent Electricity System Operator, we believe that the use of Criterion B 5 may be useful in facilitating review of further requirements by the stakeholders.

Comment

WECC disagrees with the use of Criterion B 2 because data and evidence collection is necessary to demonstrate compliance.

Response

The P81 SDT believes that this concern appears to miss the essential aspect of the P81 project in its initial phase which is to retire requirements that do little to protect BES reliability. Thus, hardwiring in data retention mandatory requirements does not seem aligned with generally accepted methods of auditing or promoting an effective and efficient ERO. It is incumbent on the entities to maintain sufficient evidence to support compliance with requirements, and the P81 SDT believes that any requirements that strictly support compliance assessments without a benefit to reliability should be evaluated for revision or retirement.

Comment

WECC disagrees with Criterion B 7 because it would allow other regulators to enforce a requirement.

Response

The P81 SDT agrees with WECC's overarching concern; however, that situation exists today. If there is a requirement that is already part of a regulatory order or under the purview of another governmental authority and is consistently understood and applied across North America, then the P81 SDT believes it should remain a candidate for retirement to remove this potential for double jeopardy. It is important to note, however, that it must be consistently covered across the whole continent and mandatory so as to ensure no "gaps" exist.

Comment

Independent Electricity System Operator suggests that another word be used other then "Technical" to describe Criterion B.

Response

Based on this concern, the P81 SDT changed "Technical" to "Identifying."

C. <u>Comments of Criterion C</u>

Comment

WECC believes Criterion C 1, C 2, C 4, C 6 and C 7 all need to be made more specific or improved.

Response

The concern seems predicated on Criterion C determining whether or not to retire a requirement, which is not the intent. Instead, these criteria will be used to ensure additional pertinent information and considerations are used to assist in the determination of whether a Reliability Standard requirement satisfies both Criterion A and Criterion B. The P81 SDT shall consider these data and

reference points to make a more informed decision. Also, note that these criteria are conceptual only and were developed to assist the industry and the P81 SDT with their analysis. The P81 SDT thanks WECC for their thorough review; however, it will retain the criteria as written.

Comment

Independent Electricity System Operator states it is confusing as to how the section C, "Additional Data and Reference Points" will be used by the drafting team to determine retirement of Reliability Standards even though they have satisfied Criterion A and Criterion B.

Response

The P81 SDT believes that a review of the technical white paper, which will be issued and will contain the initial list of requirements to be retired, will promote an understanding on how Criterion C was used. Criterion C is only meant to provide additional considerations to provide further justifications that the proposed retirements do not have any other underlying reliability related need.

D. Miscellaneous Comments on Phase I vs. Subsequent Phases

Comment

ACES Power Marketing Standards Collaborators suggest that the scope of the SAR should be changed to include current standards under development.

Response

At this time it appears that including requirements from current standards under development would overly complicate the P81 project and intrude on other standard drafting teams. With that said, the P81 SDT does intend to work with and coordinate with other standard drafting teams to help ensure that new requirements are not being drafted that appear to meet the P81 criteria. Also, the P81 SDT will be working with the Standards Committee to draft guidelines to help standard drafting teams draft requirements that are more results-based, and not requirements that would meet the P81 criteria.

Comment

ERCOT indicates that the criteria used for future phases should remain flexible.

Response

The initial list should not preclude the use of additional criteria for future phases where additional criteria support the elimination of requirements in those efforts. Given the amount of commenters who requested numerous requirements be considered in future phases, it appears reasonable that P81 project should remain flexible to meet the needs of stakeholders. Thus, the P81 SDT has revised the SAR to apply to Phase I only.

Comment

SRC urges the SAR simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired.

Response

The P81 SDT did not intend for the list of requirements proposed in the draft SAR to come across as a list without flexibility.

Comment

ACES Power Marketing Standards Collaborators suggests that requirements that are assigned to the wrong functional entities should be added as a criterion for revision or retirement.

Response

The P81 SDT believes that ACES's suggestion should be considered during the development of a Phase 2 SAR. In many instances, applicability can be a complex undertaking and there may be large diversity, irrespective of an entity having some common high-level responsibilities as listed in the NERC Registry and Functional Model.

Comment

NERC staff suggests that any technical justifications that rely on Criterion B 6 should address how NAESB, etc. would handle the requirement.

Response

As a general matter, many commenters suggest that the P81 project develop thorough justifications and remain in line with the suggested Criteria. NERC staff's concern of reliance on Criterion B 6 will also be considered when developing the justifications. The P81 SDT removed references to NAESB, but notes that when relying on B 6, sufficient reference will be made to other mandatory requirements which effectively ensure there will be no gap on a continent-wide basis and in addition, what will ensure that on an ongoing basis, this gap will remain addressed by something other than a NERC standard requirement. The technical white paper will consider these concerns. In addition, the P81 SDT believes that ongoing training for drafting teams will ensure that these types of requirements are no longer developed.

Organization	Yes or No	Question 1 Comment

Organization	Yes or No	Question 1 Comment
Western Electricity Coordinating Council	No	WECC offers the following related to the criteria listed in the SAR.WECC beleives the OVERARCHING CRITERIA listed under "A" needs clarification and that as currently identified is too vague. The Overarching Criterion statement is too broad and is contrary to the FPA Section 215. "Impact" is an ambiguous term. There is no measure as to how to quantify a Requirement's "impact" and to distinguish between "little" impacts as opposed to some other metric of "impact." More importantly, however, a Requirement that has any impact on the reliable operation of the BES cannot be dismissed as inconsequential, even if it is determined to have "little" impact. The "impact" must be weighed against the "burden" of the standard and potential for efforts to demonstrate compliance hindering or preventing other more "impactful" reqiurements. Further, the Standard Requirements work in concert with one another. For many Standard Requirements, it is impossible to reasonably assess the "impact" of a single Standard Requirement. For example, the "purpose" statement for CIP Standard Requirements reads that "[CIP Standard Requirements] should be read as part of a group of standards numbered Standards CIP-002 through CIP-009." To examine the "impact" of a single Standard Requirement, therefore, contradicts the intent and purpose of many Standard Requirements that are crafted to operate in concerns with one another.WECC believes the B1 Administrative Technical Criteria needs claificaiton and is vague as currently written. The term "administrative" is ambiguous and could cover a broad range of activities. Further, "administrative requirements" often require evidence of program or procedure creation. However, WECC does agree with this criteria, but only in the case where all three criteria listed (administrative, does not support reliability, and needlessly burdensome) are met.WECC disagrees witht he B2 Technical Criteria Data Collection/Data Retention. Data Collection/Data Retention is often the only means by which a Responsible Entity can objectively demonstrate compliance. As to mandatory data retention

Organization	Yes or No	Question 1 Comment
		periods, an explicit mandate to retain data may be required to meet compliance obligations unique to a particular Standard Requirement. However, if treated correctly, a requirement for the data collection/retention for compliance purposes could be removed from the Requirmeetns and made part of the Measures or RSAWs.WECC Disagrees with the B3 criteria Purley Documentation unless it can be clearly demonstrated that the dcoumentation does not protect the reliabiltity of the BES in any way. In some cases Plans/Policies/Procedures are necessary for employees to have a guide for not only protection but maintaining and restoring BES assets (i.e. Restoration Plans). Documentation of plans, policies and procedures, is key in defining the parameters of compliance. Further, plans/policies and procedures are often the only means by which Compliance and Enforcement can assess a responsible entity's compliance with a Standard Requirement.WECC Disagrees with the B4 criteria Purely Reporting unless no purpose for the reporting can be identified. Reporting helps overarching organizations (ex. ES ISAC) detect potential issues earlier, by giving them more information and from multiple entities. These issues may seem small or insignificant when viewed by a singular entity but may have a more a drastic impact when viewed from the perspective of the entire BES. WECC Disagrees with the B5 criteria Periodic Updates unless it can be clearly demonstrated that the reproting has no operational benefit to reliability. Without these requirements there is nothing in place to ensure entityies are maintaining, and periodically verifying the accuracy of these documents. With the criteria established as it is, there is no real way of measuring the effect of "operational benefit to reliability". Is it measured by the size of impact (MW), by time (something that will take over a 1hr), or by Time Horizon (Same-Day operations vs. Real Time Operations). It is recommended to establish a more accurate means to measure these criteria. If proberly handled, these reporting requirements that that demonstrate the entities are maintaining certain necessary

Organization	Yes or No	Question 1 Comment
		documents could be moved from the Requirements to the Measures or RSAWs.WECC agrees with the B6 criteria of Business Practices.B7 criteria Redundant: Although WECC agrees requirements should not be redundant with each other, if compliance is left to other regulators (Open Access Transmission Tariff, NAESB, etc.) compliance may not be held up to NERC expectations or interpretations. In identifying redundant standards, only NERC Reliability Standards should be considered.WECC agrees with B* criteria,WECC believes the B9 criteria needs clarification and as written is vague. How will the determination that teh Requirements do little, if anything, to promote the protection of the BES be determined?WECC disagrees with C1. The FFT determination is not predicated on any particular Standard Requirement. The FFT determination is fact specific. Even a requirement that is critical to the BES may have an FFT'd violation if the manner in which the requirement was violated was minor.WECC beleives C2 is vague and needs clarification. Not certan what it means if the requirement is being revieweed in an on-going Standards Development Project. Is this the same as B7 Redundant?WECC agrees C3 is a factor that should be considered.WECC agrees with C4 but beleives information on how the tiers will be viewed should be included.WECC agrees with C5.WECC believes C6 and C7 are vague as written and believes that these last two reference points are intended to indicate that if the answer is yes, then the requirement or standard would NOT be eligable for retirement. This should be clarified.
Independent Electricity System Operator	No	(1) The IESO supports this proposed effort and agrees with most of the criteria, with some exceptions (except #5): "The Reliability Standard requirement requires responsible entities to periodically update (e.g., annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability."Take for example the system restoration plan. An annual review is necessary to ensure that the plan recognizes BES facility changes that occurred since the last review/update. Another

Organization	Yes or No	Question 1 Comment
		example is the exceptions to the cyber security policy that needs to be reviewed and approved by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Applying this criterion in a broad brush manner without looking at each requirement may result in removing requirements that are still needed for reliability.(2) Generally, the nine criteria listed in the SAR are simple and sufficient to be used to determine retirement of reliability standard requirements. It is recommended that the word "Technical" in the heading of the B section "Technical Criteria" be erased as the criteria aren't based on technical data. Also, it is unclear and confusing as to how the section C "Additional Data and Reference Points" will be used by the drafting team to determine retirement of reliability standards even though they have satisfied Criteria A and B. Criterion B.9 can potentially be deleted as its purpose seems to be the duplication of Criterion A.(3) The SAR narrative for TOP-001-1a R3 states the requirement is redundant with IRO-001-1a R8. IRO-001-1a does not exist; we believe, it should be IRO-001-1.1 R8 instead.
NERC Technical Staff Review	No	(1) Revise Criteria A to focus on the content of the Reliability Standards. NERC Staff suggests the following language for Criteria A: "The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to protect reliable operation of the BES." This language is currently included as Criteria B9. NERC notes that both Criterion B8 (hinders the protection or reliable operation of the BES) and B9 (little, if any value as a reliability requirement) are duplicative with Criterion A and should be eliminated. Since any requirement that meets Criterion B8 or B9 would necessarily meet Criterion A, this creates an unintended consequence by undermining the objective that requirements for consideration must satisfy both the overarching Criterion A and a separate technical criteria. For these reasons, NERC Staff supports the elimination of both Criteria B8 and B9 and the re-phrasing of Criteria A. (2) There is significant overlap between Criteria B3 (Purely Documentation) and B5

Organization	Yes or No	Question 1 Comment
		(Periodic Updates) and these criteria could be combined. Criteria B3 addresses requirements for entities to develop a document that is not necessary and Criteria B5 addresses the requirement for entities to periodically update such documentation. NERC Staff suggests renaming Criteria B3 "Documentation" and suggests the following language: "The Reliability Standard requirement requires responsible entities to develop and/or periodically update a document (e.g., plan, policy or procedure) which is not necessary to protect BES reliability." (3) The explanation of Criterion B6 (Commercial or Business Practice) states that the Reliability Standard requirement "is a commercial or business practice, e.g., better served as a NAESB standard or as part of NAESB Electric Industry Registry (EIR)." However, the technical justifications provided for the application of the B6 criteria do not state that the standard/requirement should be addressed in another manner, e.g., with a NAESB standard. Please clarify or otherwise modify this criterion appropriately. Further, the technical justification should address the fact that such business practices may not be applicable to the same entities and may not be mandatory or enforceable.
Northeast Power Coordinating Council	Yes	NPCC participating members support the P81 initiative and agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement. The criteria are also consistent with FERC's guidance in Paragraph 81 of the FFT Order. With respect to the words in Criterion A wording, it could be interpreted as an indication that the original reliability standard requirement was a mistake. Suggest the SDT consider alternative wording to indicate that the experience with the requirement, over time, has proven not to be useful to accomplish its initially intended reliability objective, or has not produced clear results for the initially intended reliability objective.Criterion A, and Technical Criteria B9 "Little, if any, value as a reliability requirement" are redundant.

Organization	Yes or No	Question 1 Comment
ACES Power Marketing Standards Collaborators	Yes	In general, we agree with the criteria. However, we do offer two suggestions. First, in criterion B.1, we suggest striking "and is needlessly burdensome". If the activity does not support reliability the burden is irrelevant. Second, we suggest if there are current standards under development that are already proposing to retire requirements that those requirements should be considered for inclusion in this project. In order to include those requirements, the proposed reason for retirement should align with one of the criteria in this project. This would accelerate the retirement of unnecessary requirements. Third, we suggest requirements that are assigned to the wrong functional entities should be added as a criterion for revision/retirement.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade Associations).	Yes	The Trade Associations agree with the criteria listed in the SAR to identify Reliability Standard requirements for retirement. As noted above, the criteria were the product of intense discussions among numerous stakeholders, including the Trade Associations, NERC, and the Regional Entities. The criteria are also consistent with FERC's guidance in paragraph 81 of the FFT Order.
SPP Standards Review Group	Yes	We concur that the proposed criteria are a good starting point for the evaluation of requirements to be retired.
Salt River Project	Yes	We like the criteria and methodology.

Organization	Yes or No	Question 1 Comment
SRC	Yes	The criteria listed in the SAR capture the right categories; however, consider restructuring B1. B2 through B5 are examples of administrative requirements and should possibly be sub-items of B1. While we generally support this proposed effort and agrees with most of the criteria, the exception is B5: “The Reliability Standard requirement requires responsible entities to periodically update (e.g., annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.”Take for example the system restoration plan. An annual review is necessary to ensure that the plan recognizes BES facility changes that occurred since the last review/update. Another example is the exceptions to the cyber security policy that needs to be reviewed and approved by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Applying this criterion in a broad brush manner without looking at each requirement may result in removing requirements that are still needed for reliability. In addition, the acid test for retirement of a requirement is when the standard drafting team reviews the overall reliability impact of removing a particular requirement from a standard, and how it may affect other related standards. In brief, it may be a bit premature to pass on this judgment at the SAR stage. We urge the SAR proponent to simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired. And, in order to meet the requirements for regulatory approval, we suggest the SDT to provide strong technical basis to justify each retirement.
Manitoba Hydro	Yes	The technical criteria B.9, "Little if any, value as a reliability requirement", is very subjective and should be redefined or clarified.
Georgia System Operations Corporation	Yes	Georgia System Operations agrees with the criteria listed in the SAR to identify Reliability Standard requirements for either modification or

Organization	Yes or No	Question 1 Comment
		withdrawal.
seattle city light	Yes	Seattle City Light supports the consolidated comments of the industry Trade Organizations.
NV Energy	Yes	We agree with the Overarching Criterion and the specific Technical Criteria, and believe that the types of requirements specified in the Technical Criteria can be eliminated without any impact to reliable operation of the interconnected transmission system.
Occidental Energy Ventures Corp.	Yes	Occidental Energy Ventures Corp. ("OEVC") fully supports the efforts taken by the Trades, NERC, and the Regional Entity Management Group to develop the criteria to identify requirements that may be eligible for retirement and modification. The overarching criterion is extremely important in our view, as it serves to remind us all that FERC's original purpose as defined by Section 215(a)(4) of the Federal Power Act is to oversee wide-area reliability of the bulk power system. In recent years, the Commission's authority has expanded into distribution systems and localized load shedding - important issues, but already regulated by the PUCs. In our view, this is duplicative work that increases costs without serving improved reliability.OEVC also believes that the technical criteria are appropriate and complete for now. However, in our view, Item #8 "Hinders the protection or reliable operation of the BES" and Item #9 "Little, if any, value as a reliability requirement" will need further refinement in future phases of this project. Both are quite subjective, and FERC in our opinion will only respond to fact-based quantitative data that shows that BPS reliability is not improved by a given reliability requirement. A painful reminder may be the requirement for secondary Facility Ratings (FAC-008-3) which FERC clearly perceives to be a reliability imperative despite overwhelming industry rejection of the concept. It is unlikely that this view will change unless tangible cost/benefit evidence to the contrary

Organization	Yes or No	Question 1 Comment
		is provided to the Commission.
South Carolina Electric and Gas	Yes	I support removing redundancy and any items that are not related to reliability impacts.
Georgia Transmission Corporation	Yes	Georgia Transmission Corporation agrees with the criteria listed in the SAR to identify Reliability Standard requirements for either modification or withdrawal.
Electric Reliability Council of Texas, Inc.	Yes	ERCOT agrees with the ISO/RTO SRC comments. However, in addition for SRC comments, ERCOT offers the following: ERCOT agrees with the criteria listed in the SAR to identify Reliability Standard requirements for retirement in Phase 1. However, the criteria used for future phases should remain flexible. The initial list should not preclude the use of additional criteria for future phases where additional criteria support the elimination of requirements in those efforts.
SERC EC Planning Standards Subcommittee	Yes	
Southwest Power Pool Regional Entity	Yes	
Bonneville Power Administration	Yes	
Dominion	Yes	
Pepco Holdings Inc & Affiliates	Yes	
PPL Corporation NERC Registered Affiliates	Yes	

Organization	Yes or No	Question 1 Comment
Tampa Electric Company	Yes	
City of Garland	Yes	
Entergy Services, Inc.	Yes	
Wolverine Power Supply Cooperative, Inc.	Yes	
Central Husdon Gas & Electric Corporation	Yes	
Tucson Electric Power	Yes	
American Electric Power	Yes	
Public Service Enterprise Group	Yes	
CPS Energy	Yes	
Duke Energy	Yes	
Edison Mission Marketing & Trading	Yes	
Illinois Municipal Electric Agency	Yes	
Essential Power, LLC	Yes	
Idaho Power Company	Yes	
Occidental Power Services, Inc.	Yes	

Organization	Yes or No	Question 1 Comment
City of Austin dba Austin Energy	Yes	
Transmission Agency of Northern California	Yes	
Ameren	Yes	
Kansas City Power & Light	Yes	
MidAmerican Energy Company	Yes	

2. The Initial Phase of the P81 project is designed to identify all FERC-approved Reliability Standard requirements that easily satisfy the criteria. Do you agree that the suggested list of Reliability Standard requirements included in the draft SAR easily satisfy the criteria listed in the draft SAR? If you disagree, please provide a statement supporting what Reliability Standard requirements you would add or subtract from the Initial Phase, including a citation to at least one element of Criterion B, as applicable.

Summary Consideration:

A. Support for Initial List

The majority of commenters support the initial list of requirements suggested for retirement in the draft SAR. Supporters include SPP Standards Review Group, The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC), the Canadian Electricity Association (CEA) (collectively, the Trade Associations), Salt River Project, SRC, Georgia System Operations Corporation, Seattle City Light, Duke Energy, NV Energy, Occidental Energy Ventures Corp., South Carolina Electric and Gas, Ameren, Electric Reliability Council of Texas, Inc., SERC EC Planning Standards Subcommittee, Dominion, Pepco Holdings Inc & Affiliates, PPL Corporation NERC Registered Affiliates, Tampa Electric Company, Manitoba Hydro, City of Garland, Entergy Services, Inc., Wolverine Power Supply Cooperative, Inc., Central Hudson Gas & Electric Corporation, Tucson Electric Power, CPS Energy, Edison Mission Marketing & Trading, Illinois Municipal Electric Agency, Idaho Power Company, City of Austin dba Austin Energy, Transmission Agency of Northern California, and Kansas City Power & Light. Also, the following entities appear to generally support the current list, while requesting additional requirements to be added: Georgia Transmission Corporation, Occidental Power Services, Inc., American Electric Power, and ACES Power Marketing Standards Collaborators. This level of support appears to be a testament to the hard work of the collaborative process and provides significant context in which to consider the merits of those stakeholders who requested that certain requirements be added or removed from the initial list.

B. Concerns with requirements included in the initial list

Comment

Northeast Power Coordinating Council (NPCC), Southwest Power Pool Regional Entity (SPP RE), Western Electricity Coordinating Council (WECC), NERC staff technical review (NERC staff) presented concerns with retiring requirements related to PRC-008-0 and PRC-009-0.

Response

As SRC points out, PRC-009-0 is already scheduled to be retired. More specifically, in Order No. 763 at Paragraph 103[3] the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Similarly, under Standards Development Project 2007-17 Protection System Maintenance, which recently passed stakeholders vote on August 27, 2012, PRC-008-0 is scheduled to be retired and replaced with PRC-005-2. PRC-005-2 will likely be presented to the NERC Board of Trustees in November for approval. To avoid confusion and promote regulatory efficiency, the P81 SDT intends to present PRC-008-0 and PRC-009-0 in the final SAR for informational purposes only. Accordingly, PRC-008-0 and PRC-009-0 will not be included in the P81 project for purposes of comment and ballot.

Comment

NPCC is concerned that it may only receive information related to UVLS program assessment and performance after an event if PRC-010-0 R2 and PRC-022-1 R2 are retired.

Response

The P81 SDT believes it is appropriate to retire PRC-010-0 R2 and PRC-022-1 R2 because the Regional Entities' current compliance and monitoring processes provide for the review of UVLS program assessment and performance during a spot check, compliance audit, etc., which makes PRC-010-0 R2 and PRC-022-1 R2 unnecessary. Thus, the P81 SDT believes that PRC-010-0 R2 and PRC-022-1 R2 should remain within the scope of P81 for purposes of comment and ballot.

Comment

WECC and SPP RE requested that CIP-007-3 R7.3 not be retired, based on concerns related to demonstrating compliance with other requirements.

Response

These concerns appear to miss the essential aspect of the P81 project which is to retire requirements that do little to protect BES reliability. The P81 SDT believes that data retention in and of itself has little to do with protecting BES reliability, particularly when the Regions have authority to request data to show compliance with any mandatory Reliability Standard. Thus, hardwiring in data retention into mandatory Reliability Standard requirements does not seem aligned with generally accepted methods of auditing or promoting an effective and efficient ERO compliance program. In other words, it seems to adopt the position of WECC and SPP RE on this matter could essentially be an endorsement that every Reliability Standard requirement should be accompanied with a mandatory data retention requirement, which would seem counterintuitive given the processes set for in the Compliance Monitoring and Enforcement Program. Thus, the P81 SDT believes that CIP-007-3 R7.3 should remain within the scope of P81 for purposes of comment and ballot.

[3] *Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards*, 139 F.E.R.C. ¶ 61,098 (2012).

Comment

WECC also disagrees with the inclusion of IRO-016-1 R2 with a concern that Reliability Coordinators must be required to document their actions for compliance and enforcement purposes.

Response

Reliability Coordinator actions are conducted over recorded lines or via written directives, and, thus, the documentation is already available for a Regional Entity to inspect. Further, during a spot check or compliance audit a Regional Entity has the authority to request information, as well as the entity has the burden to prove compliance – if the entity chooses to prove compliance via recorded phone lines or logs is not necessarily an appropriate subject for a mandatory Reliability Standard. Thus, the P81 SDT believes that IRO-016-1 R2 should remain within the scope of P81 for purposes of comment and ballot.

Comment

WECC and NERC staff express concerns with including MOD-004-1. Specifically, WECC states:

MOD-004 is not redundant to TOP-002 even though the CBM itself may be a tariff issue and rarely used. The reliability piece is that if the CBM is used by a TSP then the details of it must be available for use in system studies. Without the awareness of a transmission holdback for CBM when it exists, a network study could be run and show no issues but if at some time the CBM were implemented an overload could result. This might not always be the case but unless the CBM parameters are known and modeled it could impact reliability.

NERC staff suggests that MOD-004-1 may be more appropriate for a subsequent phase unless a solid technical justification can be developed for MOD-004-1 that addresses relevant FERC's ruling.

Response

One of the tenants of the initial phase of P81 is that the requirement does not need significant technical justifications or editing. Notwithstanding the apparent support for MOD-004-1 to be part of the P81 project, it is also apparent to the P81 SDT that at this time MOD-004-1 needs additional review and consideration prior to any decision to retire all or part of its requirements. It is also noteworthy that there are a large number of requests to consider other MOD standards in subsequent phases, and it is likely appropriate to consider the MOD Standards as a whole so that MOD-004-1 can be more thoroughly analyzed. For example, CBM is referenced in a number of MOD Standards, such as MOD-001-1a, MOD-008-1 and MOD-028-1. Thus, the P81 SDT has removed MOD-004-1 from the list of requirements proposed for the initial phase and MOD-004-1 will be considered in a subsequent phase of the P81 project.

Comment

WECC, Public Service Enterprise Group and Essential Power, LLC state that CIP-002-1a R4 should not be retired. WECC makes several points, including:

"An entity has many enforcement agencies to contact without the FBI listed in the operating instructions they could easily be overlooked. . . . . Retiring R4 will remove the incentive of having a working relationship with the FBI, especially among the smaller entities. Retiring R4 may effectively delay or prevent the FBI from rapidly locating those responsible for sabotage."

Also, Public Service Enterprise Group and Essential Power, LLC state:

"If the entity owns or operates a BES asset, there is a clear reliability benefit to have appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to these Law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response."

Response

The P81 SDT believes that the practices and procedures discussed by WECC, Public Service Enterprise Group and Essential Power, LLC are accomplished via R1 through R3 of CIP-002-1a, not R4. For example, consistent with R2,[4] it is common practice to contact local law enforcement authorities when there is any suspicion that sabotage has occurred at a BES facility. The entity's corporate security and site personnel will consult with local law enforcement to assess the situation and facts to determine whether a suspected or actual act of sabotage has occurred. If they find a suspected or actual act of sabotage has occurred, reliability entities as well as the Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP), as appropriate, will be contacted in accordance with R2. Thus, pursuant to R1 through R3, when there is an instance of sabotage that warrants contacting the FBI or RCMP or any other federal or national governmental authority, entities will contact them. Conversely, the requirement in R4 to establish communication contacts with the FBI or RCMP, as applicable, is purely an administrative, documentation and data collection task requirement – there is no operational or results-based aspect of R4, like there is with R1 through R3. Accordingly, in CIP-001-2a R1 through R3 serve the results-based reliability function, while R4 is a static, administrative requirement that has no direct or clear nexus to protecting BES reliability. For these reasons, the P81 SDT believes that CIP-001-2a R4 should remain within the scope of P81 for purposes of comment and ballot.

Comment

Bonneville Power Administration, WECC and NERC staff do not support the proposed retirement of TOP-001-1a R3.

[4] "**R2.** Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection."

Response

Bonneville Power Administration, WECC and NERC staff all make valid points. Although there is redundancy between TOP-001-1a R3 and IRO-001-1a R8 related to Reliability Coordinators, this redundancy was addressed in Standards Development Project 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces TOP-001-1a R3 and reads as follows:

Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued and identified as such by its Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.

TOP-001-2 has been approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, the P81 SDT intends to present TOP-001-1a R3 in the final SAR for informational purposes only. Accordingly, TOP-001-1a R3 will not be included in the P81 project for purposes of comment and ballot.

Comment

SRC and NERC staff state that VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2 should not be included in the P81 project until they have first been processed for retirement via the WECC regional standards process.

Response

SRC and NERC staff make a valid point that regional standards proposed for retirement need to first proceed through their region prior to being considered for retirement via a NERC standards development project. For these procedural concerns, VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2 have been removed from the P81 project; however, the P81 SDT encourages WECC to consider the deliberations of the collaborative process and act on retiring VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2, as appropriate.

Comment

Central Hudson Gas & Electric Corporation, Public Service Enterprise Group, and American Electric Power and Essential Power, LLC express concern with the inclusion of CIP-003-3 R4 and its sub-requirements in the P81 project. AEP states:

“AEP recommends instead that CIP-003 R1 be removed in which case CIP-003 R3 (and CIP-003 R2.4) can also be removed. However, if the drafting team does not agree with this recommendation, CIP-003 R3 must be retained in order for entities to take targeted exception(s) where applicable (for example, in circumstances where an entity’s program is more stringent than the CIP requirements).”

Public Service Enterprise Group and Essential Power, LLC indicate that “[t]he exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy.”

Response

The reason for retiring CIP-003-3, -4 R3 and its sub-requirements is directly applicable to the concerns expressed. In other words, although the CIP exception requirements have never been available for use to exempt an entity from compliance with any requirement of any NERC Reliability Standard, entities apparently are reading the CIP exception requirements out of context. These requirements only apply to exceptions to internal corporate policy, and only in cases where the policy exceeds a NERC Reliability Standard requirement or addresses an issue that is not covered in a NERC Reliability Standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of eight characters in length, and be changed every 30 days, this provision could be used for internal governance purposes to lessen the corporate requirement back to the password requirements in CIP-007 R5.3, or in conjunction with a Technical Feasibility Exception (TFE) to something else. Therefore, removal of this requirement has no effect on the TFE process or compliance with any other CIP requirement. Also, the retirement of the CIP exception requirements would not impact an entity's ability to maintain such a process within their corporate policy governance procedures. Consequently, the CIP exception requirements provide little protection for BES reliability and are an internal administrative and documentation requirement that is outside the scope of the other CIP requirements. Thus, the P81 SDT believes that CIP-003-3, -4 R3 and its sub-requirements should remain within the scope of P81 for purposes of comment and ballot.

Comment

Public Service Enterprise Group and Essential Power, LLC also request the P81 project not include EOP-004-1 R1 because it will soon be replaced by EOP-004-2.

Response

The P81 SDT notes that the past ballot of EOP-004-2 did not pass and it is currently in the balloting stage. The P81 SDT has coordinated its efforts with the chair of Project 2009-01 and both agree there is no conflict between retiring EOP-004-1 R1 and the direction of Project 2009-01. At such time that the EOP-004-2 project does obtain stakeholder approval and is scheduled for NERC Board of Trustees review, P81 SDT will reconsider the need to include EOP-004-1 R1. Thus, at this time, the P81 SDT believes that EOP-004-1 R1 should remain within the scope of P81 for purposes of comment and ballot.

Comment

Public Service Enterprise Group and Essential Power, LLC further request that FAC-002-1 R2 be removed from the P81 project based on the concern that the three year study retention requirement could be increased to six years via compliance and monitoring data retention.

Response

The concern of Public Service Enterprise Group and Essential Power, LLC, however, appears to miss the essential aspect of the P81 project in its initial phase which is to retire requirements that do little to protect BES reliability. Thus, hardwiring in data retention

mandatory requirements does not seem aligned with generally accepted methods of auditing or promoting an effective and efficient ERO compliance program. Accordingly, the P81 SDT believes that FAC-002-1 R2 should remain within the scope of P81 for purposes of comment and ballot.

Comment

NERC staff questioned the inclusion of FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 in the P81 project. Specifically, NERC staff states:

"These requirements, combined with others, provide checks and balances on the Facility Rating Methodology and Transfer Capability methodology established by the responsible entities. This provides a reliability benefit by requiring the responsible entity to consider areas in which their methodology may not be sufficient to support reliable operation of the interconnected transmission system. There may be better ways of assuring that entities have sufficient methodologies and alternatives should be considered during Phase II. NERC Staff suggests that the SDT reconsider whether discussing the methodology (and not the numerical rating of a facility) has commercial or market related implications. With respect to FAC-013-2 R3, NERC Staff suggests that the SDT reconsider whether the requirement relates to "a back and forward on transfer capability" as noted in the draft SAR, as the requirement pertains only to the methodology for determining transfer capability."

Response

The P81 SDT notes that Page 5 of NERC's Standards Process Manual states:

"A Reliability Standard includes a set of Requirements that define specific obligations of owners, operators, and users of the North American Bulk Power Systems. The Requirements shall be material to reliability and measurable."

It appears difficult to read into the plain language of FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 specific obligations that are material to reliability and measurable or provide more than a little amount of protection to BES reliability. For instance, in practice, while the owners of ratings and transmission capability methodologies have made these documents available for comment during the duration of the mandatory Reliability Standard regime, experience shows that little, if any, technical comments have not been submitted on these documents. In the regional processes, entities are on a variety of committees and have professional relationships, and, therefore, if they have a concern with a methodology, they have ample opportunity to seek out professional technical critique as a best practice. FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 seem toonly formalize a vehicle for professional technical critique without an exacting nexus between it and reliability. Given that entities that develop these methodologies must comply with rigorous requirements in FAC-008 and FAC-013, the P81 SDT believes that the addition of a mandatory best practice technical critique process does not seem necessary, material or measurable. It is also noteworthy that there is no obligation for any entity to request a methodology nor is there any obligation on the owner of the methodology to respond to any

comments with any level or burden of technical thoroughness. Thus, the P81 SDT believes that FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 should remain within the scope of P81 for purposes of comment and ballot.

C. Suggested additions to the initial list

Comment

NPCC suggests adding FAC-003-1 R3, FAC-003-1 R4, CIP-005-3 R4, and CIP-007-3 R8.

Response

While the P81 SDT believes there appears to be merit in considering the FAC-003 and CIP requirements suggested by NPCC, these requirements were discussed in the collaborative process and it was generally agreed that these requirements need additional technical review prior to any consideration of retirement. Thus, these requirements will be considered in a subsequent phase of the P81 project.

Comment

NPCC and SRC suggest adding IRO-014-2 R2 and it sub-requirements. According to NPCC, these requirements are administrative requirements only and do not enhance reliability, while SRC states that these requirements satisfy Criterion B1 and Criterion B5.

Response

While IRO-014-2 R2 seems like a valid candidate for P81, it is not a FERC-approved Reliability Standard. At this time, it has been adopted by the NERC Board of Trustees and has yet to be filed with FERC for approval. As the P81 project matures or a more formalized approach to P81 is adopted by NERC in its Rules of Procedures or processes, the consideration of Reliability Standards not yet approved may be practical. However, at this time, the scope of the P81 project remains FERC-approved Reliability Standards. The exception to this is if a FERC-approved requirement being proposed for retirement is duplicated in a standard that has only been adopted by the NERC Board of Trustees. Thus, at this time, IRO-014-2 R2 is not ripe for consideration in P81.

Comment

ACES Power Marketing Standards Collaborators suggests adding FAC-010-2.1 R5 and FAC-011-2 R5 in the initial phase for the following reasons:

"FAC-010-2.1 R5 is an administrative requirement for the Planning Authority to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The PC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments. This requirement meets Criteria B.1 and B.9.(7) FAC-011-2 R5 is an administrative requirement for the Reliability Coordinator to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The RC is already required to distribute its methodology in R4."

Response

ACES Power Marketing Standards Collaborators' position is similar to the reasons that FAC-008-1 R2, FAC-008-1 R3, FAC-008-3 R4, FAC-008-3 R5 and FAC-013-2 R3 were included in the draft SAR as satisfying the criteria and appropriate for retirement. Further, the language in all of these Reliability Standard requirements is very similar. Thus, the P81 SDT has added FAC-010-2.1 R5 and FAC-011-2 R5 to the initial phase of P81.

Comment

ACES Power Marketing Standards Collaborators suggests that IRO-005-3 R11 is redundant with MOD-028-1 R6.1, MOD-029-1a R3, and MOD-030-2 R2.4 and that the MOD standards already require the Transmission Service Provider to consider IROLs and SOLs when determining Available Transfer Capability/Available Flowgate Capability and Total Transfer Capability. Specifically, IRO-005-3 R11 reads:

"The Transmission Service Provider shall respect SOLs and IROLs in accordance with filed tariffs and regional Total Transfer Calculation and Available Transfer Calculation processes."

Response

It appears that while IRO-005-3 R11 may be redundant for the reasons stated by ACES Power Marketing Standards Collaborators; however, this requirement has been retired in IRO-005-4, which was approved by the Board of Trustees and is pending a filing at FERC. Thus, recognizing that that Project 2006-06 Reliability Coordination has already received many of the necessary approvals to retire IRO-005-3 R11, it does not seem to serve regulatory efficiency to include IRO-005-3 R11 in the P81 project as well. Thus, the P81 SDT did not add IRO-005-3 R11 to the initial phase of P81.

Comment

ACES Power Marketing Standards Collaborators suggests COM-001-1.1 should be retired because English is the dominant language used.

Response

To retire such a requirement would possibly need coordination with the Canadian authorities in French speaking provinces and those in areas of the United States were Spanish is a first language. Such coordination would seem to complicate the retirement of COM-001-1.1, and, thus, the P81 SDT believes it is more appropriately considered in a subsequent phase.

Comment

With regard to VAR-001-2 R5, ACES Power Marketing Standards Collaborators states that it:

". . . is redundant with FERC's pro forma tariff and was originally included in the NERC policies to align them with said tariff. The requirement compels the PSE and LSE to arrange for reactive resources to satisfy the reactive requirements of the Transmission Service

Provider. PSEs and LSEs cannot purchase transmission service without purchasing reactive service or demonstrating to the transmission provider that they have arranged for reactive resources. From a practical perspective, this means they always purchase reactive service from the Transmission Provider. Furthermore, it is the Transmission Operator that actually ensures reactive resources are dispatched per VAR-001-2 R2."

Response

The P81 SDT notes that when approving VAR-001, in Order No. 693 at Paragraph 1858,[5] the Commission recognized:

". . . that all transmission customers of public utilities are required to purchase Ancillary Service No. 2 under the OATT or self-supply, but the OATT does not require them to provide information to transmission operators needed to accurately study reactive power needs. The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities."

ACES Power Marketing Standards Collaborators states VAR-001-2 R5 appears to be redundant with Ancillary Service No. 2 under the OATT. Moreover, VAR-001-2 R5 is very limited to this OATT obligation and regional process, and, therefore, does not speak to the Commission's concern related to providing information to Transmission Operators for accurate reactive power studies. Therefore, it appears that VAR-001-2 R5 satisfies the P81 criteria by doing little to protect BES reliability and being redundant with the OATT. Thus, the P81 SDT has added VAR-001-2 R5 to the initial phase of P81.

Comment

ACES Power Marketing Standards Collaborators also suggests adding BAL-002 R1, BAL-002 R3, BAL-005-0.1b R1 and its sub-requirements, INT-004-2 R1, and TOP-005-2a R3.

Response

The P81 SDT notes that during the collaborative process the linkage between the BAL and INT standards was discussed and there seems to be merit considering whether some BAL and INT standards could be combined. The Trade Associations, among others, suggested this be conducted in a subsequent phase of P81. Given the complexity related to the linkage between the BAL and INT standards, along with TOP-005-2a R3, the P81 SDT believes that additional review should be conducted in a subsequent phase of P81 prior to retiring the suggested BAL and INT standards.

Comment

[5] VAR-001-2 was approved via a Letter Order issued on January 10, 2011.

ACES Power Marketing Standards Collaborators also suggests including PRC-011-0 R2, PRC-015-0 R3, PRC-016-0.1 R3, PRC-017-0.1 R2, PRC-021-0.1 R2, PRC-023-1 R2, and PRC-023-2 R3. American Electric Power suggests the following additions: PRC-021-1 R2; PRC-018-1 R5; PRC-016-0.1 R3; PRC-015-0 R3; PRC-011-0 R2; PRC-007-0 R3; CIP-006 R1.5; CIP-004-3 R4; CIP-007 R5.1.1; CIP-007 R5.1.3; CIP-007 R6.3; CIP-007 R6.4; CIP-003-3, CIP-003-4 R1; CIP-003-3, CIP-003-4 R1.2; CIP-003-3, CIP-003-4 R1.3; CIP-003-3, CIP-003-4 R2.4; CIP-003-3, CIP-003-4 R3. Tampa Electric recommends that the P81 SDT ensure that the CIP requirements proposed for removal via P81 are also removed from v5 of the NERC CIP standards. Tampa Electric also supports the consideration of the following for NERC CIP standards: (1) Removal of data collection requirements (CIP-005-3a,-4a R5.3, CIP-006-3c,-4c R7 and R8.3, CIP-007-3,-4 R5.1.2, R6.4and R7.3, CIP-008-3,-4 R2); and (2) Removal of annual review requirements (CIP-002-3,-4 R4, CIP-003-3,-4 R1.3, R4.3, R5.1.2, and R5.3, CIP-006-3c,-4c R1.8, CIP-007-3,-4 R9, and CIP-009-3,-4 R1).

Response

There was much discussion around the PRC and CIP standards during the collaborative process. There are several issues that impact the retirement of these requirements including not creating a reporting gap by retiring PRC standards and the coordination of CIP standards with the Version 5 SDT. Given these complications, the P81 SDT believes it is best to consider these CIP and PRC Standards as part of a subsequent phase of the P81 project. To address Tampa Electric's other concern, the P81 SDT has been coordinating its activities with the CIP Version 5 SDT, and will continue to do so, so that the agreed upon retirements do not reemerge in CIP Version 5.

Comment

Occidental Power Services, Inc. requests the removal of the PSE function from the applicable sections of the following: INT-001-3 R1, INT-004-2 R2, IRO-001-1.1 R3, IRO-001-1.1 R8, IRO-005-3 R10, TOP-005-2 R3, and VAR-001 R5. ACES Power Marketing Standards Collaborators also suggests removing PSE and LSE the applicable sections of IRO-005-3 R10.

Response

The removal of applicable from the requirements is an interesting suggestion that would take some more technical review and modification of the requirements. Thus, the P81 SDT believes this suggestion is more appropriate for consideration in a subsequent phase of P81.

Comment

Georgia Transmission Corporation suggests the following additions: MOD-016-1.1 R1, MOD-016-1.1 R1.1, MOD-016-1.1 R3, MOD-017-0.1 R1, MOD-017-0.1 R1.1, MOD-017-0.1 R1.2, MOD-017-0.1 R1.3, MOD-017-0.1 R1.4, MOD-018-0 R1, MOD-018-0 R1.2, MOD-018-0 R1.3, MOD-018-0 R2, MOD-019-0.1 R1, MOD-020-0 R1, MOD-021-1 R1, MOD-021-1 R2, MOD-021-1 R3, PRC-005-1b R2, PRC-005-1b R2.1, PRC-005-1b R2.2, PRC-006-1 R7, PRC-006-1 R8, PRC-006-1 R14, PRC-007-0 R2, PRC-007-0 R3, PRC-011-0 R2, PRC-015-0 R3, PRC-017-0 R2, PRC-018-1 R5, PRC-021-1 R2, PRC-023-1 R3.3, and TOP-001-1a R4.

Response

Georgia Transmission Corporation points out many of the same requirements that the trade associations suggest for subsequent phases of the P81 project. As mentioned above, for example, we are deferring the consideration of MOD-004-1 to a subsequent phase so it may be considered in the context of other MOD Standards. The P81 SDT believes it is more appropriate to consider Georgia Transmission Corporation's suggestions in a subsequent phase.

Comment

South Carolina Electric and Gas asked if the measures associated with requirements being proposed for retirement would be modified or removed as well.

Response

The relevant measures and other associated elements will be marked as retired in the standard. These will be identified in the redlines of the standards that will be posted with the requirements during the next comment period.

Comment

ERCOT states that the justification statement for BAL-005-0.1b R2 could benefit from additional clarification regarding how it is redundant with BAL-001 R1 and R2 and the justification for EOP-009-2 R2 should also be enhanced.

Response

The P81 SDT notes that additional clarification for BAL-005-0.1b R2, EOP-009-0 R2 and other requirements will be included in the technical white paper being developed by the P81 SDT.

In summary, of the initial list in the draft SAR, MOD-004-1, VAR-002-WECC-1 R2 and VAR-501-WECC-1 R2 have been deferred to a subsequent phase. Of the suggested additions, it appears that only VAR-001-2 R5, FAC-010-2.1 R5 and FAC-011-2 R5 satisfy the P81 criteria without significant technical review, and, thus, are appropriate to be added to the final SAR for the initial phase. As a general note, any requirements suggested for the initial phase, but not adopted, shall be considered by the P81 SDT in a subsequent phase of the project, and, therefore, the entities do not need to resubmit the requirements.

Organization	Yes or No	Question 2 Comment
Northeast Power Coordinating Council	No	From page 25 of the SAR, "Since PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 provides little protection to the BES and better handled under event analysis and lessons learned papers, it should be removed." is not valid due to that fact that as of this posting the Event Analysis Program (EAP) has not become part of the RoP and is therefore a voluntary program. The requirements that are covered by these standards are mandatory cannot be replaced by a voluntary program. Refer to the following:Additionally, the EAP process is an after-the-fact Analysis of an event or events. These standard requirements (PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2) address different needs which can be determined only if such an event occurs. For example, from PRC-008-0--"R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance." This requirement addresses the need to have an equipment maintenance and testing program in place prior to an event. Discovering that an entity did not have this as a result of an event analysis would, in this case, be after the damage is done and would not serve reliability. Analyzing why the UFSL program did not operate properly would come under the purview of the EAP but that is different from the Standard's intent. PRC-008-0--"R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days)." If the EAP was relied upon to meet this requirement the receipt or confirmation of this program would only occur after an event. PRC-009-0--"R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall

Organization	Yes or No	Question 2 Comment
		analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:R1.1 A description of the event including initiating conditions.R1.2 A review of the UFLS set points and tripping times.R1.3 A simulation of the event.R1.4 A summary of the findings."Although this Standard appears that it could be covered under EAP, it is a highly detailed technical study and needs to be carried out on its own accord. Event Analysis will focus primarily what caused the event that triggered the UFLS program but not necessarily the program itself. Because of the importance of the UFLS program to the reliability of the system, its performance should not be analyzed only on a voluntary basis and not only by those entities that actually shed load as a result of the event, but against the whole regional program.PRC-009-0--"R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event."This is administrative, refer to the response for R1 preceding. PRC-010-0--"R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days)." This should not triggered only after an event, see preceding response for R1 preceding. PRC-022-1--"R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request."This is the same situation as for the UFLS program. Refer to the responses preceding. IRO-014-2 --The following requirements in Standard IRO-014-2 are administrative requirements only and do not enhance reliability, and should be considered for removal in the Initial

Organization	Yes or No	Question 2 Comment
		Phase. "R2. Each Reliability Coordinator shall maintain its Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 as follows: [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]2.1. Review and update annually with no more that 15 months between reviews. 2.2. Obtain written agreement from all of the Reliability Coordinators required to take the indicated action(s) for each update.2.3. Distribute to all Reliability Coordinators that are required to take the indicated action(s) within 30 days of an update."FAC-003-1 Requirements R3, and R4 (shown below) and their sub-requirements are administrative (reporting) requirements only and do not enhance reliability, and should be considered for removal in the Initial Phase. R3. The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.R4. The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions taken by the RRO as a result of any of the reported outages.In addition, as shown below, CIP-005-3 R4 and CIP-007-3 R8 are essentially the same. Suggest to eliminate CIP-005-3 R4 and include assessment of access points in CIP-007-3 R8.CIP-005-3 R4:"R4. Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following: R4.1. A document identifying the vulnerability assessment process; R4.2. A review to verify that only ports and services required for operations at these access points are enabled; R4.3. The discovery of all access points to the Electronic Security Perimeter; R4.4. A review of controls for default accounts, passwords, and network management community strings; R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan." CIP-007-3 R8:"R8. Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the

Organization	Yes or No	Question 2 Comment
		following: R8.1 A document identifying the vulnerability assessment process; R8.2 A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled; R8.3 A review of controls for default accounts; and, R8.4 Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan."
Southwest Power Pool Regional Entity	No	SPP RE does not agree that PRC-008 R1 and R2 should be retired or that they provide "little protection to the BES and [are] better handled under event analysis and lessons learned papers". UFLS equipment maintenance and testing programs ARE important to BES reliability, in a preventative mode, and are NOT covered under the Event Analysis process. Preventative maintenance is very important to reliability; without it, events are more likely. Industry should not wait for an event to happen to collect information and consider maintenance and testing. UFLS is the last line of "defense in depth protection of the BES" (Criteria C6). SPP RE's comment follows the discussion around removing PRC-005 and its relationship to BES reliability.SPP RE does not agree that CIP-007-3 R7.3 should be retired. R7.3 requires the Responsible Entity to maintain records of how data storage media was erased or destroyed prior to disposal or redeployment of the Cyber Asset (which could be simply the media previously removed from the Cyber Asset). In the absence of such records, the Responsible Entity cannot demonstrate compliance with CIP-007-3 R7.1 and CIP-007-3 R7.2, rendering those requirements not auditable. Elimination of this requirement could also result in a loss of visibility of Cyber Assets that have been disposed of or redeployed, also hampering the ability of the Responsible Entity to demonstrate compliance and the Compliance Enforcement Authority to audit compliance with the remaining requirements.
Bonneville Power Administration	No	BPA does not support the proposed retirement of TOP-001-1a R3. BPA does not agree that TOP-001-1a R3 is redundant with IRO-001-1a R8 because IRO-001-1a R8 only addresses RC directives, whereas TOP-001-1a R3 addresses both RC directives and TOP directives. BPA believes that retiring TOP-001-1a R3 before TOP-001-2 R1 is

Organization	Yes or No	Question 2 Comment
		effective would create a gap because no requirement would address TOP directives. BPA supports the additional proposed retirements and thanks the drafting team for their efforts.
ACES Power Marketing Standards Collaborators	No	(1) We believe there are other requirements that easily meet the criteria. (2) VAR-001-2 R5 is redundant with FERC's pro forma tariff and was originally included in the NERC policies to align them with said tariff. The requirement compels the PSE and LSE to arrange for reactive resources to satisfy the reactive requirements of the Transmission Service Provider. PSEs and LSEs cannot purchase transmission service without purchasing reactive service or demonstrating to the transmission provider that they have arranged for reactive resources. From a practical perspective, this means they always purchase reactive service from the Transmission Provider. Furthermore, it is the Transmission Operator that actually ensures reactive resources are dispatched per VAR-001-2 R2. Thus, VAR-001-2 R5 satisfies criteria B.1, B.6, B.7, and B.9.(3) BAL-002 R1 and R3 are redundant. R1 compels the BA to have access to and operate Contingency Reserve to respond to disturbances. R3 requires the BA to activate sufficient Contingency Reserve to comply with DCS. We suggest removing R1 because it is redundant (Criterion B.7). This applies to both versions 0 and 1 of the standard.(4) BAL-005-0.1b R1 and its sub-requirements are not necessary. All generation, transmission and load is currently contained within the metered boundaries of a BA. It is impossible to add new generation, transmission and load and not be within the metered boundaries of a BA. To do so, would require the equipment owner to carve out an area from the BA. For example, if a TO added a new transmission line, it would have to put a meter on both ends to carve it out of any BA footprint. In the process, they, in effect, create a new BA. The only way these requirements can't be met would be if BAs started removing metering equipment en masse. Given removing metering equipment has significant financial consequences due to inaccurate energy accounting; it is not going to happen. Thus, it meets Criterion B.9. Furthermore, TOs are already required to identify metering requirements in FAC-001-0 R2.1.6 as part of its facility connection requirements. It also meets Criterion B.7.(5) COM-001-1.1 is unnecessary and the audit of it has

Organization	Yes or No	Question 2 Comment
		largely become a demonstration that it is an administrative requirement. English is the primary language across the vast majority of the Interconnections under NERC's purview and it is the primary language in all of the areas under FERC's jurisdiction. For the few companies in areas where English is not predominant, those companies will be unable to meet other requirements if they use a different language to speak with companies from predominantly speaking English languages. Furthermore, audits have regulated this to predominantly an administrative requirement. The auditors largely look for statement that the English language is required despite the fact that all evidence has been provided in English, observations of control center conversations have shown English is used, and the audit has been conducted in English. If there is a need for this requirement, it should be relegated to a regional requirement for those regions that include areas that do not speak predominantly English. Thus, this requirement meets Criteria B.1 and B.9.(6) FAC-010-2.1 R5 is an administrative requirement for the Planning Authority to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The PC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments. This requirement meets Criteria B.1 and B.9.(7) FAC-011-2 R5 is an administrative requirement for the Reliability Coordinator to respond to comments on its SOL methodology. Failure to provide a written response to technical comments does not impact reliability. The RC is already required to distribute its methodology in R4. Any functional entity that would have provided technical comments will see any adjustments when they receive the methodology. This requirement meets criteria B.1 and B.9.(8) INT-004-2 R1 has nothing to do with reliability and should be included in the list of retirements. Failing to reload an Interchange Transaction that was curtailed for a reliability event has no reliability impact. It is a remnant from the NERC Policies that was added at the request of market participants because once transactions were cut, reliability entities did not always allow the transaction to resume once the reliability issue had been addressed. This is strictly a commercial issue. Thus, this requirement meets Criterion B.9.(9)

Organization	Yes or No	Question 2 Comment
		IRO-005-3 R10 should be modified to reflect the functional model. In cases where there are differences in derived limits, PSEs and LSE cannot operate to the most limiting parameters. They are not in a position to even have information on the parameters such as facility ratings. Rather, their role is to follow directives. Thus, inclusion of PSE and LSE in the requirement does not support reliability. Thus, this requirement meets Criterion B.9. (10) IRO-005-3 R11 is redundant with MOD-028-1 R6.1, MOD-029-1a R3, and MOD-030-2 R2.4. The MOD standards already require the TSP to consider IROLs and SOLs when determining Available Transfer Capability/Available Flowgate Capability and Total Transfer Capability. This requirement meets Criterion B.7. (11) PRC-011-0 R2 should be retired. A requirement is not needed to compel the TO and DP to provide data on its UVLS equipment maintenance program to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(12) PRC-015-0 R3 should be retired. A requirement is not needed to compel the TO, GO and DP to provide data on their Special Protection Systems (SPS) to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(13) PRC-016-0.1 R3 should be retired. A requirement is not needed to compel the TO, GO and DP to provide data on their SPS Misoperations analyses and corrective action plans to the Regional Entity. The Regional Entity's CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(14) PRC-017-0.1 R2 should be retired. A requirement is not needed to compel the TO, GO and DP to provide documentation of the SPS maintenance and testing program to the Regional Entity. The Regional Entities CMEP and NERC's Rules of Procedure compel the TO, GO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(15) PRC-

Organization	Yes or No	Question 2 Comment
		021-0.1 R2 should be retired. A requirement is not needed to compel the TO and DP to provide UVLS program data to the Regional Entity. The Regional Entities CMEP and NERC's Rules of Procedure compel the TO and DP to provide information regarding enforceable requirements per the Regional Entity's request. This requirement meets Criteria B.1, B.4, and B.9.(16) PRC-023-1 R2 and PRC-023-2 R3 are redundant with FAC-008-1 R1.2.1 and FAC-008-3 Part 2.4.1. FAC-008-1 R1.2.1 and FAC-008-3 Part 2.4.1 already require the GO and TO to consider relay protective devices when determining facility ratings. The DP cannot limit the Facility Rating because a DP does not have Transmission Facilities. They only have relays that impact Facility Ratings that must ultimately be considered by the TO. This requirement meets Criterion B.7(17) TOP-005-2a R3 is redundant with the INT standards and should be retired. In the NERC Functional Model, the only role for the PSE is to facilitate Arranged Interchange. The INT standards already govern Arranged Interchange and contain the necessary information that the PSE must provide. Furthermore, Project 2007-03 Real-Time Operations has proposed retirement of this requirement as it is redundant with NAESB e-Tag specifications. Beyond the E-tag data there is no additional information that a PSE or LSE could provide for the BA or TOP to conduct operational assessments. This requirement meets Criteria B.6, B.7 and B.9.(18) PRC-006-1 R7 should be retired. Failure by a Planning Coordinator to provide data to another Planning Coordinator within 30 days is not a reliability issue because Planning Assessments have long time lines to complete the studies. Furthermore, any failure to provide data within 30 calendar days is most likely a simple oversight. If a Planning Coordinator refuses to provide data, the requesting Planning Coordinator may get involved and which will compel them to provide the data. This can be done without the need for this requirement. This requirement meets criterion B.4.
Western Electricity Coordinating Council	No	WECC supports the majority of the Standards Requirements identified, but notes concerns with the following. WECC recommends eliminating CIP-003 R1 in its entirety.WECC disagrees with the inclustion of CIP-007, R7.3. This requirement is necessary for entity's to demonstrate compliance with the other sub-requirements of CIP 007 R7. However, this requirement could be moved to a Measure or RSAW to

Organization	Yes or No	Question 2 Comment
		demonstrate compliance with the other sub-requirements of CIP-007, R7.WECC disagrees with the includsion of IRO-016-1, R2. Required documentation of the RC's actions to remedy an event is necessary for quality and efficient root cause analysis, including insight into the RC's wide view of actions during an event or disagreement. The language in the SAR statement for IRO-016-1 R2 points to this information being monitored through Spot Checks or other compliance monitoring methods. If this standard is removed yet the information is to be included in future compliance monitoring there must be some sort of methodology that requires the entity to retain the associated data to be kept for the duration of the required cycle for monitoring (i.e. audit cycle if monitored through audits). It is important that entities document the actions taken that analyze the effect on the system as well as the BES for either an even or/and for the disagreement on the problem. Therefore, it is important that this information is part of the overall compliance monitoring program.MOD-004 is not redundant to TOP-002 even though the CBM itself may be a tariff issue and rarely used. The reliability piece is that if the CBM is used by a TSP then the details of it must be available for use in system studies. Without the awareness of a transmission holdback for CBM when it exists, a network study could be run and show no issues but if at some time the CBM were implemented an overload could result. This might not always be the case but unless the CBM parameters are known and modeled it could impact reliability.WECC disagrees with the recommendations with PRC-008-0 R1 and PRC-008-0 R2. Unless these standards are being superseded, WECC does not agree that they provide "little protection to the BES." They are not administrative in nature like the other standards in this group. They insure that maintenance and testing program is established and implemented for an entity's UFLS protection systems. Without these standards, there is reduced assurance that UFLS protection systems will operate correctly when called upon for an under-frequency event. UFLS has a vital role in its effectiveness for preserving system stability and elimination of these standards may reduce its effectiveness. This standard is about making sure the equipment is maintained not about collecting data. If and when PRC-005-2 is adopted, and if it were to include the UFLS devices, then this standard should be

Organization	Yes or No	Question 2 Comment
		considered for removal.WECC believes the statements associated with TOP-001-1a, R3 are incorrect. Removing TOP-001-1a would result in no NERC requirement for parties to follow TOP directives. The current TOP-001-1a R3 requires BOTH TOP and RC directives to be followed. The proposed IRO-001-3 R2 requires ONLY RC directives to be followed. In addition, the SAR statement is incorrect. TOP-001-1a R3 applies to directives issued by the TOP (and also the RC). IRO-001-1a applies only to directives from the RC. If the intent, as they state, is to replace TOP-001-1a R3 with IRO-001-3, that leaves a void for an entity to comply with a directive from the TOP. Only the part about following an RC directive is redundant. Requirement should be modified to eliminate the redundancy, but not retired. WECC disagrees witht he inclusion of CIP-001, R4. An entity has many enforcement agencies to contact without the FBI listed in the operating instructions they could easily be overlooked. This Requirement has encouraged entities to establish a current communication line with the FBI. In fact, several other larger entities are members of InfraGardÂ®, which is a partnership between the FBI and the private sector. Retiring R4 will remove the incentive of having a working relationship with the FBI, especially among the smaller entities. Retiring R4 may effectively delay or prevent the FBI from rapidly locating those responsible for sabotage. The requirement is not “needlessly burdensome”, which is a criteria for deletion.WECC believes the requirements VAR-002-WECC-1, R2, and VAR-502-WECC-1, R2, are probably the best way of demonstrating compliance with the accociated R1 requirments. The two VAR R2 requirements do not say the entity has to submit the information to WECC (Regional Entity), only that it shall have the documentation to prove exclusion for the sub requirements in R1. We’ve had cases where entities don’t meet the 98% availability and if the entity was claiming exclusion time, WECC would want to review the documentation that proves the exclusion. It is in the entity’s best interest to keep exclusion documentation in case its units don’t make the 98%, but this is beter suited for a Measure or RSAW.
Independent Electricity System Operator	No	(1) We generally agree that most of the identified standards/requirements would meet the proposed criteria. However, as indicated under Q1, we believe that the “annual review” criterion is too broad which could result in retiring some

Organization	Yes or No	Question 2 Comment
		requirements that are still needed for reliability. In addition, the acid test for retirement a requirement is when the standard drafting team reviews the overall reliability impact of removing a particular requirement from a standard, and how it may affect other related standards. In brief, it is premature to pass on this judgment at the SAR stage. We urge the SAR proponent to simply suggest that the proposed requirements be considered and evaluated by the SDT as opposed to making a presumption (and hence setting a high expectation for the industry) that the proposed list will be retired. And, in order to meet the requirements for regulatory approval, we suggest the SDT to provide strong technical basis to justify each retirement.
American Electric Power	No	AEP does not disagree with a majority of the requirements proposed by the drafting team, though we recommend the team reconsider the inclusion of CIP-003 R3 and associated sub-requirements. AEP recommends instead that CIP-003 R1 be removed in which case CIP-003 R3 (and CIP-003 R2.4) can also be removed. However, if the drafting team does not agree with this recommendation, CIP-003 R3 must be retained in order for entities to take targeted exception(s) where applicable (for example, in circumstances where an entity's program is more stringent than the CIP requirements).AEP would like the team to consider the following additional Reliability Standard requirements as candidates for retirement on this initial, or subsequent, request for comment. Standard: PRC-021-1Requirement: R2Requirement Text: Each Transmission Operator and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.Criterion: B4,9Standard: PRC-018-1Requirement: R5Requirement Text: The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.Criterion: B2Standard: PRC-016-0.1Requirement: R3Requirement Text: The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).Criterion: B4Standard: PRC-015-0Requirement:

Organization	Yes or No	Question 2 Comment
		R3Requirement Text: The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of Studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).Criterion: B4Standard: PRC-011-0Requirement: R2Requirement Text: The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days).Criterion: B4Standard: PRC-007-0Requirement: R3Requirement Text: The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days).Criterion: B4Standard: CIP-006Requirement: R1.5Requirement Text: Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.Criterion: B7Standard: CIP-007Requirement: R5.1.1Requirement Text: The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.Criterion: B7Standard: CIP-007Requirement: R5.1.3Requirement Text: The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.Criterion: B7Standard: CIP-007Requirement: R6.3Requirement Text: The Responsible Entity shall maintain logs of system events related to cyber security, where technically Feasible, to support incident response as required in Standard CIP-008-3.Criterion: B7Standard: CIP-007Requirement: R6.4Requirement Text: The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.Criterion: B1, B3Standard: CIP-003-3, CIP-003-4Requirement: R1Requirement Text: Cyber Security Policy - The Responsible Entity shall document and implement a cyber security policy that represents

Organization	Yes or No	Question 2 Comment
		management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:Criterion: B1, B3, B7, B9Standard: CIP-003-3, CIP-003-4Requirement: R1.2Requirement Text: The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. Criterion: B1, B3, B7, B9Standard: CIP-003-3, CIP-003-4Requirement: R1.3Requirement Text: Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2. Criterion: B5Standard: CIP-003-3, CIP-003-4Requirement: R2.4Requirement Text: The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy. Criterion: B7Comment: Although AEP does not necessarily agree with removal of this requirement (see R3 comment below), R2.4 is redundant with R3.3 (which is being removed) and should probably be removed along with R3.Standard: CIP-003-3, CIP-003-4Requirement: R3 (R3.1, R3.2, R3.3)Requirement Text: Exceptions - Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). Criterion: Comment: If R1 is not removed, R3 (or some exception process) is necessary. For example, if the Cyber Security Policy goes above and beyond the standards, then an exception may be needed even though the standards are met.
Public Service Enterprise Group	No	For these requirements, KEEP:CIP-001-2a R4. If the entity owns or operates a BES asset, there is a clear reliability benefit to have appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to these Law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response. Thus we feel that this requirement should be kept within the standards.CIP-003-3 R3. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. It's removal may have a negative impact on the industry. CIP-003-4 R3. The exceptions language in R3, though

Organization	Yes or No	Question 2 Comment
		rarely used, allows for those instances where an entity is unable to conform with it's cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. It's removal may have a negative impact on the industry. TOP-005-2a R1. "TOP-003-2 requires operating entities such as GOs and TOs to provide operating data to BAs ands TOPs. In TOP-005-2a, R2 and R3 requires BAs and TOPs to exchange this data with other BAs and TOPs . R1 requires BA and TOP recipients of such data to execute a confidentiality agreement so that its confidentiality is protected. This requirement ultimately protects the confidentiality of data provided by entities under TOP-003-2.For these requirements, KEEP BUT MODIFY:FAC-002-1 R2. We believe the three year limitation on documentation sets a limit; otherwise six years may be required (the period between audits. We do suggest removing the language " and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days)." because we see no reliability benefit.For these rerquirements, KEEP UNTIL REPLACED:EOP-004-1 R1. NERC's Event Analysis Process was approved by NERC's BOT on February 9, 2012. This process has already been adopted as RFC's process under EOP-004-1, R1. Draft standard EOP-004-2 will replace Regional reporting requirements in R1 with consistent NERC-wide requirements; however, while the draft does not presently require the use of the NERC Event Analysis Process, that process is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. Keep until these NERC ROP changes are approved by FERC and become effective.PRC-008-0 R1. This is required for reliability. Such a testing program has been incorporated into draft PRC-005-2 When this is adopted, PRC-008-0 can be retired.PRC-009-0 R1. The NERC Event Analysis Process is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. Keep until these NERC ROP changes are approved by FERC and become effective.PRC-009-0 R1.1. See R1 above.PRC-009-0 R1.2. See R1 above.PRC-009-0 R1.3. See R1 above.PRC-009-0 R1.4. See R1 above.
Essential Power, LLC	No	CIP-001-2a, R4. This requirement should be removed from the Paragraph 81 project. If an entity owns or operates a BES asset, there is a clear reliability benefit to have

Organization	Yes or No	Question 2 Comment
		appropriate law enforcement contacts and procedures to address sabotage or other security incidents. Similarly, the federal agencies feel that this is a good idea. In a coordinated attack environment, sabotage reporting to these law enforcement agencies from the BES operators and owners would improve the ability of a coordinated response. Thus we feel that this requirement should be kept within the standards.CIP-003-3, R3. This requirement should be removed from the Paragraph 81 project. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform to its cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. Its removal may have a negative impact on the industry.CIP-003-4, R3. This requirement should be removed from the Paragraph 81 project. The exceptions language in R3, though rarely used, allows for those instances where an entity is unable to conform to its cyber security policy. In addition, the requirement has been approved by the industry and FERC more than once. Its removal may have a negative impact on the industry.EOP-004-1, R1. This requirement should be removed from Phase 1 of the Paragraph 81 project, until replaced by EOP-004-2. NERC's Event Analysis Process was approved by NERC's BOT on February 9, 2012. This process has already been adopted as RFC's process under EOP-004-1, R1. Draft standard EOP-004-2 will replace Regional reporting requirements in R1 with consistent NERC-wide requirements; however, while the draft does not presently require the use of the NERC Event Analysis Process, which is embedded in proposed NERC ROP changes filed with FERC on May 7, 2012. This requirement should be kept until these NERC ROP changes are approved by FERC.FAC-002-1, R2. This requirement should be removed from the Paragraph 81 project, and modified instead. We believe the three year limitation on documentation sets a limit; otherwise six years may be required (the period between audits). We do suggest removing the language “and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days)." because we see no reliability benefit to this element of the requirement.
Occidental Power Services,	No	OPSI recommends the following additions for Phase 1 implementation: 1. INT-001-3, R1. The Load Serving, Purchasing-Selling Entity shall ensure that Arranged

Organization	Yes or No	Question 2 Comment
Inc.		Interchange is submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.Criteria: B6, B9Statement: This requirement is at best a business practice of markets (protocol). These schedules can be rejected if not correctly submitted, can be cut if not executed correctly, and the PSE can be penalized if there are offenses.Recommendation: Remove PSE from R1 and from the Applicability section.2. INT-004-2, R2. The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:o R2.1 The average energy profile in an hour is greater than 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than Â±10%o R2.2 The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than Â±25 megawatt-hourso R2.3 A Reliability coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons. Criteria: B6,B9Statement: This requirement is at best a business practice of markets (protocol). These schedules can be rejected if not correctly submitted, can be cut if not executed correctly, and the PSE can be penalized if there are offenses.Recommendation: Remove PSE from R2 and from the Applicability section.3. IRO-001-1.1, R3 and R8.R3. The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing- Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes.R8. Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the

Organization	Yes or No	Question 2 Comment
		Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.Criteria: B9Statement: PSEs do not generally receive Reliability Directives from RCsRecommendation: Remove PSE from R3 and R8 and from the Applicability section.4. IRO-005-3, R10. In instances where there is a difference in derived limits, the Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall always operate the Bulk Electric System to the most limiting parameter.Criteria: B9Statement: PSEs do not generally derive limits for the transmission of power over the BES.Recommendation: Remove PSE from R10 and from the Applicability section.5. TOP-005-2, R3. Each Purchasing-Selling Entity shall provide information as requested by its Host Balancing Authorities and Transmission Operators to enable them to conduct operational reliability assessments and coordinate reliable operations.Criteria: B6,B9Statement: PSEs have to supply this information as a requirement for participating in market functions.Recommendation: Remove PSE from R3 and from the Applicability section.6. VAR-001, R5. Each Purchasing-Selling Entity shall arrange for (self-provide or purchase) reactive resources to satisfy its reactive requirements identified by its Transmission Service Provider.Criteria: B6,B9Statement: This is a requirement to participate in competitive markets (generally, it is included in the transmission rate) or is required by tariffs in non-competitive markets. The PSE has no option but to purchase the reactive power in order to make the transaction.Recommendation: Remove PSE from R5 and from the Applicability section.
Georgia Transmission Corporation	No	GTC agrees that the suggested list easily satisfies the criteria in the draft SAR, but GTC also believes this is an incomplete list for Phase I. GTC also believes the following Reliability Standard requirements easily satisfy the criteria listed in the draft SAR and recommends reconsidering and adding to the list in the initial Phase I.MOD-016-1.1;R1:The Planning Authority and Regional Reliability Organization shall have

Organization	Yes or No	Question 2 Comment
		documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses. [Meets Criteria A, B1, B2, B3, B9]MOD-016-1.1 R1.1 The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values. Meets Criteria A, B1, B3, B4, B9MOD-016-1.1 R3 The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and Load-Serving Entities that work within its Planning Authority Area. Meets Criteria A, B1, B3, B9MOD-016-1.1 R3.1 The Planning Authority shall make this distribution within 30 calendar days of approval. Meets Criteria A, B1, B3, B9MOD-017-0.1 R1 The Load-Serving Entity, Planning Authority and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R1. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.1 Integrated hourly demands in megawatts (MW) for the prior year. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.2 Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.3 Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years. Meets Criteria A, B1, B4, B9MOD-017-0.1 R1.4 Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested. Meets Criteria A, B1, B4, B9MOD-018-0 R1 The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or

Organization	Yes or No	Question 2 Comment
		dispersed basis) shall: Meets Criteria A, B1, B3, B9MOD-018-0 R1.1 Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and Meets Criteria A, B1, B3, B9MOD-018-0 R1.2 Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load. Meets Criteria A, B1, B3, B9MOD-018-0 R1.3 Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1. Meets Criteria A, B1, B3, B9MOD-018-0 R2. The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days). Meets Criteria A, B1, B4, B9MOD-019-0.1 R1. The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-1_R 1. Meets Criteria A, B1, B4, B9MOD-020-0 R1. The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days. Meets Criteria A, B1, B4, B9MOD-021-1 R1. The Load-Serving Entity, Transmission Planner and Resource Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed. Meets Criteria A, B1, B3, B9MOD-021-1 R2. The Load-Serving Entity, Transmission Planner and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy

Organization	Yes or No	Question 2 Comment
		for Load in the data reporting procedures of Standard MOD-016-0_R1. Meets Criteria A, B1, B3, B9MOD-021-1 R3. The Load-Serving Entity, Transmission Planner and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B9PRC-005-1b R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include: Meets Criteria A, B1, B3, B9PRC-005-1b R2.1. Evidence Protection System devices were maintained and tested within the defined intervals. Meets Criteria A, B1, B3, B9PRC-005-1b R2.2. Date each Protection System device was last tested/maintained. Meets Criteria A, B1, B3, B9PRC-006-1 R7. Each Planning Coordinator shall provide its UFLS database containing data necessary to model its UFLS program to other Planning Coordinators within its Interconnection within 30 calendar days of a request. Meets Criteria A, B1, B4, B9PRC-006-1 R8. Each UFLS entity shall provide data to its Planning Coordinator(s) according to the format and schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. Meets Criteria A, B1, B4, B9PRC-006-1 R14. Each Planning Coordinator shall respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the following:14.1. UFLS program, including a schedule for implementation 14.2. UFLS design assessment 14.3. Format and schedule of UFLS data submittal Meets Criteria A, B1, B3, B9PRC-007-0 R2. The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a

Organization	Yes or No	Question 2 Comment
		UFLSprogram database. Meets Criteria A, B1, B4, B9PRC-007-0 R3. The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days). Meets Criteria A, B1, B3, B4, B9PRC-011-0 R2. The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B4, B9PRC-015-0 R3. The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days). Meets Criteria A, B1, B4, B9PRC-017-0 R2. The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days). Meets Criteria A, B1, B3, B4, B9PRC-018-1 R5. The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years. Meets Criteria A, B1, B2, B3, B9PRC-021-1 R2. Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request. Meets Criteria A, B1, B4, B9PRC-023-1 R3.3. The Planning Coordinator shall provide a list of facilities to its Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within 30 days of the establishment of the initial list and within 30 days of any changes to the list. Meets Criteria A, B1, B4, B9TOP-001-1a R4. Each Distribution Provider and Load-Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory

Organization	Yes or No	Question 2 Comment
		requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions. Same requirement as R3 which made the Phase I list, only difference is applicability.
NERC Staff Technical Review	No	After further review, NERC Staff recommends that the SDT review the following standard requirements and consider moving them from Phase I to Phase II. If the SDT determines the following standard requirements still fall into Phase I, a more robust technical justification would be needed.(1) FAC-008-1 R2, R3, FAC-008-3 R4, R5 and FAC-013-2 R3: These requirements, combined with others, provide checks and balances on the Facility Rating Methodology and Transfer Capability methodology established by the responsible entities. This provides a reliability benefit by requiring the responsible entity to consider areas in which their methodology may not be sufficient to support reliable operation of the interconnected transmission system. There may be better ways of assuring that entities have sufficient methodologies and alternatives should be considered during Phase II. NERC Staff suggests that the SDT reconsider whether discussing the methodology (and not the numerical rating of a facility) has commercial or market related implications. With respect to FAC-013-2 R3, NERC Staff suggests that the SDT reconsider whether the requirement relates to "a back and forward on transfer capability" as noted in the draft SAR, as the requirement pertains only to the methodology for determining transfer capability.(2) PRC-008-0 R2: Maintenance and testing of underfrequency load shedding (UFLS) relays is necessary to assure reliable operation of a UFLS program and this requirement is included in PRC-005-2 as part of Project 2007-17, Protection System Maintenance and Testing. NERC Staff recommends that the language in R2 relating to implementing its UFLS equipment maintenance and testing program remain to avoid a reliability gap prior to the effective date of PRC-005-2. NERC Staff recognizes that the second part of R2 does meet the criteria in the SAR and recommends that the SDT consider revising the requirement in a future phase to remove the language that requires an entity to "provide UFLS maintenance and testing program results to

Organization	Yes or No	Question 2 Comment
		its Regional Reliability Organization and NERC on request (within 30 calendar days)." (3) TOP-001-1a R3: The technical justification states that this requirement is redundant with IRO-001-1a R8. NERC Staff notes that the requirement is only partially redundant until IRO-001-3 is approved by FERC and therefore, it is premature to consider it for Phase I; it should be considered for Phase II.(4) MOD-004-1: NERC Staff notes that there are a number of Commission directives associated with MOD-004-1 and the technical justification provided for the elimination of this standard should directly address these directives. If a solid technical justification cannot be made, NERC Staff suggests that the requirements should not be included in Phase I. In addition to the above, NERC Staff recommends that the SDT consider removing the following standard requirements from the scope of the P81 project:(1) PRC-008-0 R1: The requirement to have a maintenance and testing program for UFLS is necessary to assure reliable operation of a UFLS program and this requirement is included in PRC-005-2 as part of Project 2007-17, Protection System Maintenance and Testing. NERC Staff recommends retaining R1 to avoid a reliability gap prior to the effective date of PRC-005-2.(2) PRC-009-0 R1: Analysis to assess the performance of UFLS equipment and program effectiveness following system events provides a reliability benefit by identifying whether the UFLS program is effective and whether modifications are necessary. A requirement similar to R1 is included in FERC-approved standard PRC-006-1 and NERC Staff recommends retaining R1 to avoid a reliability gap prior to the effective date of PRC-006-1. If the SDT believes this requirement is not necessary, the justification for removing R1 should discuss Commission comments in Order No. 763 pertaining to Requirement R11 in PRC-006-1.(3) VAR-002-WECC-1 and VAR-501-WECC-1: NERC Staff notes that the regional standards should be removed from the scope of the P81 project because they must first be eliminated via the regional standards development process prior to being processed through the NERC standard development process.
MidAmerican Energy Company	No	FERC Order 706 clearly states that an exception forms alternative obligations for the responsible entity to meet the requirements; an exception is not an exemption from the requirements. We believe a Responsible Entity should still be allowed to have

Organization	Yes or No	Question 2 Comment
		exceptions to its cyber security policy. MidAmerican Energy Company agrees with the proposed removal of CIP-003-3 (CIP-003-4) R3, R3.1, R3.2, R3.3, as long as CIP-003-3 (CIP-003-4) R2.4 remains and allows for possible exceptions to a Responsible Entities' cyber security policy. R2.4 states "The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy." When removing requirements eligible for TFEs, revisions to the Rules of Procedure Appendix 4D - Procedures for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards will be necessary. For example, CIP-005-3, R2.6 should be deleted from the list of requirements with TFEs in the Scope section on page 1 if the requirement is removed as part of this process.
SPP Standards Review Group	Yes	From our review of the list we feel that this is again, a good starting point, but would hope that the drafting team could add or subtract requirements as needed as Phase 1 of the project develops.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade Associations).	Yes	The Trade Associations agree with the suggested list of Reliability Standard requirements contained in the SAR for the Initial Phase of P81.

Organization	Yes or No	Question 2 Comment
Salt River Project	Yes	Yes
SRC	Yes	o PRC-009-0 R1 - R2 are in the process of being retired by PRC-006-1 as such these requirements will eventually go away. o VAR-002-WECC-1 R2 - Regional standards/requirements for retirement should go through the regional standards process not the NERC continent wide process. o VAR-501-WECC-1 R2 - Regional standards/requirements for retirement should go through the regional standards process not the NERC continent wide process. o Consider adding IRO-014-2 R2 requirements: R2 Each Reliability Coordinator shall maintain its Operating Procedures, Operating Processes, or Operating Plans identified in Requirement R1 as follows: [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]2.1. Review and update annually with no more that 15 months between reviews. 2.2. Obtain written agreement from all of the Reliability Coordinators required to take the indicated action(s) for each update.These meet criteria B1 and B5.
Georgia System Operations Corporation	Yes	Georgia System Operations agrees with the suggested list of Reliability Standard requirements contained in the SAR for the Initial Phase of P81.
seattle city light	Yes	Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Duke Energy	Yes	The initial phase of the P81 project should contain only requirements that can quickly gain industry and regulatory support and that there is adequate time to prepare a strong technical justification for. Duke Energy asks the P81 Standards Drafting Team to ensure these parameters are taken into consideration as the list is finalized, and move to a subsequent phase any requirements that could take additional time to develop a strong technical justification and consensus for.

Organization	Yes or No	Question 2 Comment
NV Energy	Yes	Our review of the rationale for each of the suggested requirements of the draft SAR supports the conclusion that these requirements should be subject to retirement.
Occidental Energy Ventures Corp.	Yes	OEVC believes that the phased approach proposed in the SAR is prudent and likely the most effective. Only the most obvious candidates for retirement or modification should be presented at this early date. If the industry moves too-far, too-fast, the result may be a blanket rejection of every proposal. Once FERC is comfortable that the industry is in-tune to their sense of risk - which includes public perception of their oversight effectiveness - we believe they will be prepared to deal with requirements that seem important on the surface, but whose contribution to reliability is illusory.
South Carolina Electric and Gas	Yes	Will the measures associated with requirements that are up for retirement be modified or removed?Eg. Removing R2 of a standard but not removing the text in M1 which refers to R2 of that same standard.
Ameren	Yes	We appreciate the excellent work done by the P81 Project team in developing the criteria and agree with the list of suggested standards/requirements that easily satisfy the criteria in this initial phase.
Electric Reliability Council of Texas, Inc.	Yes	ERCOT agrees with the ISO/RTO SCR comments. However, in addition to the SRC comments, ERCOT offers the following:ERCOT agrees that all the requirements included in the SAR warrant retirement based on the relevant criteria, as supported by the corresponding justification statements. ERCOT offers the following additional comments related to the justification statements for the SDT's consideration:BAL-005-0.1b R2 - The justification statement could benefit from additional clarification regarding the reason why this requirement is redundant, because it isn't readily apparent why this is redundant with BAL-001 R1 and R2. Maintaining CPS requires the use of regulation. Therefore, it is implicit that the relevant functional entities have regulation to comply with BAL-001 R1 and 2. Also, the justification should clarify the point of the discussion related to equating compliance based on

Organization	Yes or No	Question 2 Comment
		compliance of BAL-001 R 1 and 2 and how that argument justifies retirement. CIP-001-2a R4 - The justification statement should clarify that this requirement is redundant to the communications obligations in R1-3.CIP-003-3, 4 R1.2 - In addition to the justifications presented in the SAR, the term "readily available" is ambiguous and creates the opportunity for the use of CEA subjective judgment during compliance assessments. This is problematic for compliance risk generally, but is especially problematic when the requirement is administrative in nature. Entities should not be subject to unnecessary compliance risk based on ambiguity that can result in subjective compliance determinations based on the opinion of CEA personnel, as opposed to the four corners of the requirements, especially when the underlying requirement provides no reliability value. Further evidence that this requirement serves no purpose is the fact that it is not included in CIP v5. CIP-003-3 R3, 3.1, 3.2 and 3.3 - In addition to the justifications presented in the SAR, this issue is already fully addressed in the TFE process in Appendix 4D of the ROP, which is not only adequate, but is the appropriate place for this type of administrative function related to documentation. There are a specific set of defined requirements that allow an exception, and those exceptions have be to be filed according to the TFE process. Thus, the requirements proposed for retirement are redundant to that process. CIP-003-3, -4 R4.2 - In addition to the justification presented in the SAR, the phrase "based on sensitivity", is ambiguous and creates the opportunity to insert subjective judgment into compliance assessments. This is problematic for compliance risk generally, but especially when the requirement is administrative in nature AND redundant. Entities should not be subject to unnecessary compliance risk based on ambiguity resulting in subjective compliance determinations, as opposed to the four corners of the requirements, especially when the underlying requirement provides no operational reliability value. Further evidence that this requirement serves no purpose is the fact that it is not included in CIP v5. CIP-005-3a, -4a R2.6 - The justification statement could benefit from additional clarification as to why the banner is not useful. An appropriate use banner has not been useful over time, because people who intend to use sites inappropriately will simply ignore the

Organization	Yes or No	Question 2 Comment
		banner. Banners are generally considered to be a legal protection and not a security protection. Further evidence that this requirement serves no purpose is the fact that it has been removed from CIP v5 because the use of banners does not meet a reliability objective.CIP-007-3, -4 R7.3 - In addition to the justification presented in the SAR, it should be noted that to demonstrate that an entity performed the data destruction under R7.1 and R7.2, the entity needs to collect evidence. Having a separate requirement for evidence is redundant and not needed. COM-001-1.1 R6 - In addition to the justification presented in the SAR, the justification statement could note that this policy should be documented in the ROP for information within NERCNet that is considered sensitive or impacting to the BES. It should be a voluntary best practice or business practice for other information so that entities may use it, or use some other policy that better fits its circumstances. The justification should state that the NERCNet policy should be a voluntary best practice type of issue for information that is not considered sensitive or impacting to the BES. EOP-009-0 R2 - This is a reporting obligation and a documentation issue. The justification statement should also note that both documentation and reporting on this does not rise to the level of a reliability standard. The statement could note that this may be a best practices issue, but just for documentation. Reporting test results to REs isn't a best practice. Additionally, the justification should not state that the relevant information is better considered / obtained during an audit. If it's not relevant to the mandatory requirements, then it has no place in CMEP proceedings.FAC-002-1 R2 - The justification should not include that the relevant information is better considered / obtained during an audit. If it's not relevant to the mandatory requirements, then it has no place in CMEP proceedings.FAC-008-1 R1.3.5 - In addition to the justification presented in the SAR, the justification statement could note that the term "other assumptions" is ambiguous and introduces the potential for inefficient/ineffective administration of the CMEP due to introduction of subjectivity and opinions into compliance assessments. This is problematic for compliance risk generally, but especially when the requirement is administrative in nature AND redundant. Entities should not be subject to unnecessary compliance risk based on ambiguity resulting in

Organization	Yes or No	Question 2 Comment
		subjective compliance determinations, as opposed to the four corners of the requirements, especially when the underlying requirement provides no operational reliability value.FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5 - In addition to the justification presented in the SAR, the justification statement could note that it is inappropriate for entities other than the owners of equipment to establish facility ratings. The owners don't have to change their ratings, but the scheme is far more effective if the respective functional roles are distinct and not blurred by the review process contemplated in the requirements proposed for retirement. The owners should set the ratings and the RCs receive them and perform their functions in accordance with those ratings. The RC should not be involved with the TO/GO business-management of their equipment. Also, by keeping the roles distinct, it mitigates any liability risk of the third party if the owner uses its input and then the equipment breaks because of the new rating;FAC-013-2 R3 - Same comment as above.MOD-004-1 R1; MOD-004-1 R1.1; MOD-004-1 R1.2; MOD-004-1 R1.3; MOD-004-1 R2; MOD-004-1 R3; MOD-004-1 R3.1; MOD-004-1 R3.2; MOD-004-1 R4; MOD-004-1 R4.1; MOD-004-1 R4.2; MOD-004-1 R5; MOD-004-1 R5.1; MOD-004-1 R5.2; MOD-004-1 R6; MOD-004-1 R6.1; MOD-004-1 R6.2; MOD-004-1 R7; MOD-004-1 R8; MOD-004-1 R9; MOD-004-1 R9.1; MOD-004-1 R9.2; MOD-004-1 R10; MOD-004-1 R11; MOD-004-1 R12; MOD-004-1 R12.1; MOD-004-1 R12.2; MOD-004-1 R12.3 - ERCOT agrees with the comments/justifications.PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 - In addition to the justification presented in the SAR, the justification statement could note that the tasks required in these standards are administrative/documentation/reporting in nature and they don't affect reliability from a standards perspective. These could either be best practices or evidentiary in RSAWs - e.g. provide UFLS/UVLS program documentation - which could be relative to requirements that have actionable UVLS/UFLS requirements;TOP-001-1a R3 - ERCOT agrees with the justification with regard to the RC function, but the TOP standard also requires BAs/GOPs to follow the directives of the TOP, so the two relevant requirements are not apples to apples. Modification to one or the other

Organization	Yes or No	Question 2 Comment
		may be needed to ensure appropriate authority and corresponding obligation to follow that authority is reflected in one or the other standard, or both, but eliminate overlaps.TOP-005-2a R1 - ERCOT agrees with the justification. This should either be in the ROP or just via the ISN access process/agreement.VAR-002-WECC-1 R2; VAR-501-WECC-1 R2 - ERCOT agrees with the justification, but if the documentation/reporting are not relevant for the requirement, then the SAR should not suggest the REs should seek the info in CMEP proceedings, which should solely focus on compliance with the substance of the standards.
SERC EC Planning Standards Subcommittee	Yes	
Dominion	Yes	
Pepco Holdings Inc & Affiliates	Yes	
PPL Corporation NERC Registered Affiliates	Yes	
Tampa Electric Company	Yes	
Manitoba Hydro	Yes	
City of Garland	Yes	
Entergy Services, Inc.	Yes	
Wolverine Power Supply Cooperative, Inc.	Yes	
Central Husdon Gas & Electric	Yes	

Organization	Yes or No	Question 2 Comment
Corporation		
Tucson Electric Power	Yes	
CPS Energy	Yes	
Edison Mission Marketing & Trading	Yes	
Illinois Municipal Electric Agency	Yes	
Idaho Power Company	Yes	
City of Austin dba Austin Energy	Yes	
Transmission Agency of Northern California	Yes	
Kansas City Power & Light	Yes	

3. The subsequent phases of the P81 project are designed to identify all FERC-approved Reliability Standard requirements that could not be included in the Initial Phase due to the need for additional analysis or an editing of language. Please list any Reliability Standard requirements that you believe should be revised or retired in a subsequent phase, and include a brief supporting statement and citation to at least one element of Criterion B for each requirement listed.

Summary Consideration:

The P81 SDT is very appreciative of the time and effort the commenters spent developing their responses to Question 3. The commenters proposed numerous requirements for consideration in a subsequent phase, including requirements in BAL, CIP, INT, FAC, MOD, and PRC Reliability Standards, among others. As a general observation, the commenters suggested several ways to handle Reliability Standard requirements in the subsequent phases, including (i) retiring a requirement; (ii) modifying the requirement; (iii) changing the functional applicability of a requirement; and (iv) combining requirements or standards. Also, several commenters, such as ERCOT, Independent Electricity System Operator and SPP Standards Review Group requested the ability to raise additional Reliability Standard requirements during the subsequent phases. Given the level of interest in the subsequent phases of the P81 project, it is appropriate for the P81 SDT to carefully consider how best to propose a process for the subsequent phases. To some extent, ERCOT said it well:

"The SDT should establish a prospective process that provides adequate time and opportunity for entities to perform a meaningful review of remaining requirements to determine which additional requirements warrant retirement and to develop appropriate criteria, if relevant, that may be incremental to the ones proposed in this SAR, and to develop appropriate retirement justifications based on the relevant retirement criteria."

Consequently, while all the requests for consideration of Reliability Standard requirements in subsequent phases will receive consideration (including those requirements suggested for Phase I, but deferred to a subsequent phase), the process by which that consideration will be undertaken needs to be developed in light of the requirements suggested for subsequent phases. Accordingly, based on the comments, the P81 SDT intends to develop and suggest options to the Standards Committee in the near future on how to move forward with the subsequent phases.

Organization	Yes or No	Question 3 Comment
ACES Power Marketing		(1) EOP-002-3 R6 and R7 and their sub-requirements are redundant with BAL-001-

Organization	Yes or No	Question 3 Comment
Standards Collaborators		0.1a R1 and R2 and BAL-002 R4. BAL-001-0.1a R1 compels a BA to meet CPS1. BAL-001-0.1a R2 compels a BA to meet CPS2. BAL-002 R4 compels a BA to respond meet the DCS for all reportable events less than MSSC. EOP-002-3 R6 and R7 do not make the BA any more or less responsible to meet these requirements but rather creates an opportunity for double jeopardy. Furthermore, EOP-002-3 R6 and R7 do not make any sense in context with the CPS1 and CPS2 calculations. They are averages over a long term and would never require the emergency actions listed in the sub-requirements to comply with them. These requirements have already proven to incent behavior that is contrary to reliability (criterion B.8). At the August NERC BOT meeting, the NERC OC Chair explained that a BA shed load to meet the DCS criterion even though there were no other concerns (i.e. voltage, frequency, IROL or SOL violations) on the transmission system at the time. These requirements meet criterion B.7. (2) EOP-004-1 R2 should be considered for future retirement. The approval of the Event Analysis Procedure obviates the need for a standard requirement to analyze Bulk Electric System disturbances. This would be especially true if the procedure is added to the Rules of Procedure as NERC has planned. This requirement meets criterion B.7.(3) Retirement of FAC-001-0 R3 should be considered in the next phase. There is an implied obligation for the TO to update its Facility connection requirements when they change. Additionally, a requirement to make them available to the Regional Entity and users of the transmission system is unnecessary. First, the Regional Entity could request them through the compliance monitoring process. Second, the TO will provide the Facility connection requirements to those with genuine interconnection requests because the TO will want its connection standards met. This requirement meets criterion B.4, B.7 and B.9. (4) FAC-002-1 R1 should be revised to reflect the NERC Functional Model because it assigns the requirements to the wrong functional entities. The Transmission Planner and Planning Coordinator are responsible for conducting the assessments for new Facilities. The requirement appears to be an attempt to require the GO, TO, DP, and LSE to coordinate with the TP and PC. However, the requirement actually defines what is required in the TP and PC assessments which unfortunately place these

Organization	Yes or No	Question 3 Comment
		responsibilities on the GO, TO, DP and LSE. None of these functional entities have the capability to meet requirements such as performing dynamics studies. This requirement meets criterion B.8. (5) VAR-001-2 R2 and TOP-006-2 R2 are duplicate requirements. VAR-001-2 R2 compels the TOP to acquire sufficient reactive resources. TOP-006-2 R2 requires the RC, TOP and BA to monitor reactive resources. Since VAR-001-2 R2 applies all the time, a TOP cannot know they have acquired and maintained reactive resources unless they are monitoring them. Furthermore, TOP-006-2 R2 incorrectly applies to the BA. According to the NERC Functional Model, the BA cannot monitor reactive resources that are not generators and have no role in ensuring system voltages. Thus, TOP-006-2 R2 meets criterion B.7 because it is redundant, and it meets criteria B.8 and B.9 because it assigns responsibility to a functional entity (BA) that cannot meet it. This distracts the BA from its reliability mission.
Independent Electricity System Operator		(1) IRO-004-2 R1 could be retired if the wording in IRO-001-1.1 R8 was changed to cover all operating timeframes (Criterion B7). (2) We do not have any other particular standards/requirements in mind at this time. However, we will review and propose additional candidates for future phases as this project gets into the mid or end of Phase I. We believe the industry should focus on the Phase I effort at this time to gauge the regulator's and industry's reaction before marching too far down the path.
Western Electricity Coordinating Council		CIP 002 R2/R3/R4: Redundant and require revision. Each of these requirements requires an annual review of the Critical Asset list and Critical Cyber Asset list. WECC agrees these protections are required, however, the standard should be revised so either CIP 002-3 R4 is removed and CIP 002-3 R1-R3 are revised to require annual review and approval of the appropriate documentation, or CIP 002-3 R2 and R3 are revised to no longer require an annual review.CIP 005 R1.5/006 R3: These are redundant and should be removed/revised. CIP 006-3 R3 is redundant with CIP 005-3 R1.5. Either CIP 005-3 R1.5 should be revised to no longer require the protections of CIP 006-3 R3, or CIP 006-3 R3 should be removed and the content of CIP 006 R3 moved to CIP 005 R1.5.CIP 005 R1.5/006 R2.2: Redundant. Should be revised. Devices

Organization	Yes or No	Question 3 Comment
		applicable to these requirements may be redundant if they are classified as CCA (thus duplicated with CIP 002 - CIP 009) or reside within an ESP (thus duplicated with CIP 007). The requirements should be revised to take into account the situation where a device resides within an ESP or is classified as CCA, and is a device used in the EACM/PACM of ESPs/PSPs. Note: It appears this is being addressed in V.5 of CIP.CIP-005, R5: Should be removed and the protections highlighted in this requirement moved to appropriate requirements it references. This will cause less confusion with entities, and be more precise with exactly what documentation is required to be reviewed and approved.CIP 005 R5.1/R5.2: Redundant. Should revise CIP 005 R1.6 to include the wording of CIP 005 R5.1, and remove CIP 005 R5.1. This will cause less confusion with entities, and be better aligned with the CIP 005 R1.6 requirement.CIP 005 R5.3: Redundant. Should revise CIP 005 R3 to include the wording of this sub-requirement, and CIP 005 R5.3 should be removed. This change will create a better fit in the appropriate requirement, and be less confusing for entities.CIP 007 R9: Should be removed and the protections highlighted in this requirement moved to appropriate requirements it references. Thus CIP 007 requirements that require documentation should include the need to review and update the documentation. This will cause less confusion with entities, and be more precise with what documentation is required to be reviewed and approved.EOP-004-1 R3.2: Little, if any, value as a reliability requirement. This requirement points to attachments that could be addressed in the main part of the R3 standard. This requirement does nothing to promote the protection of the BES.VAR-001-2 R10: Redundant. The reliability purpose for R10 is to make sure that operators don't think that exceeding an SOL or IROL due to voltage issues is acceptable. There are multiple standards requiring operators not exceed and maintain an SOL or IROL with 30 minutes, regardless of the cause of the exceedance. These standards are TOP-001-2 R7, R11; TOP-004-2 R1; TOP-007-0 R2; TOP-008-1 R1.
Entergy Services, Inc.		CIP-006 R5 - A revision to the language in CIP-006 R5 is needed in order to require the review and handling of incidents of unauthorized access (when a door, gate or window has been opened without authorization), as opposed to what is more

Organization	Yes or No	Question 3 Comment
		accurately characterized as "unsuccessful" access attempts (e.g. invalid access card swipes). There currently is no definition of "unauthorized access attempts". The methods to be used for monitoring that are listed in the requirement, however do list: "Alarm Systems that alarm to indicate a door, gate or window has been opened without authorization". This method does not indicate that the alarm system must alarm on card swipes that do not result in the door opening, and be characterized as "Unauthorized Access attempts". Unsuccessful card swipes at a PSP access point, for example, do not suggest an unauthorized access attempt. A card swipe can be unsuccessful for a number of reasons, all of which are recorded by the key card system, such as the use of a deactivated card, an invalid card format, and a card not in the card file. An unsuccessful card swipe itself is not an indication that a PSP access point was “opened within authorization” because it does not indicate that the door has been opened in any manner. However, in the FAQ guidance for the CIP Reliability Standards, NERC acknowledged that Responsible Entities can consider single failed access attempts such as a single failed log-in not to be suspicious events requiring a response A single failed card swipe should be treated in the same way. The rewording of this requirement would address Criteria B-8 - "Hinders the protection or reliable operation of the BES." Investigating and documenting each unsuccessful card swipe would take a tremendous amount of time and produce a significant amount of paperwork without providing any additional physical security.CIP-005 R3 and CIP-006 R5 - Revisions to the wording around the timing of monitoring both physical and electronic access are needed. CIP-005 R3 - Monitoring Electronic Access states that "The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week." and CIP-006 R5 -Monitoring Physical Access stats that "The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in

Organization	Yes or No	Question 3 Comment
		Requirement CIP-008-3.The "twenty-four hours a day, seven days a week" portion of these requirements provides an unachievable requirement for 100% uptime for all systems used to monitor such access. The requirement should allow for a resonable amount of downtime. Either the "twenty-four hours a day, seven days a week" wording in these requirements could be removed altogether, or alternative langauge, such as requiring "High Availability" (for example 99.9% uptime) or some other wording that allowed for very small amounts of downtime that might be required for system reboots or minor maintenance.
SRC		Consider including the following standards for review in Phase II:BAL-004-0 - Time Error CorrectionMOD-030-2 - Flowgate MethodologyPRC-006-1 R8 (provision of data)PRC-006-1 R14 (administrative - response to written comments)
MidAmerican Energy Company		Consider the list provided by EEI.
Georgia System Operations Corporation		EOP-002-3, R1PER-001-0.1, R1Criteria B7, 9Statement: reference to BA or RC responsibilities and authority are within the criteria of NERC's Functional Model and so this is redundant. In addition, it is understood that these functions are substantial if not paramount for an entity to become certified as such. FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. All INT standardsCriteria B 1, 3 and 6Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Reliability Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Note: INT-007-1 R1.2 is part of Initial Phase. All data collection requirementsCIP-005-3a, 4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4; R7.3CIP-008-3, -4 R2PRC-018-1, R5Criteria B1,2 and 9Statement: These requirements are for data retention and although the need is

Organization	Yes or No	Question 3 Comment
		substancial, i.e. as a sort of forensic tool, they serve no function to reliability from an immediate time perspective.Standards currently requiring reporting.Criteria 1, 4 and 9EOP-002-3 R9.2EOP-004-1 R3 and its subrequirements; R4 and R5FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Statement: These are all reporting requirements; they do not aid reliability from an immediate time perspective. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards.Requirements applied to annual reviewsCriteria B1, 2,3 7 and 9CIP-002-2, -4 R4CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Statement: These requirements do not closely relate to operations of the Bulk Electric System. They would be better served as processes expected of entities to manage their compliance programs and processes. PRC-005-1b, R2Criteria B4, 9Statement: This requirement needs to be revised such that language is elminated as it refers to the entity providing to its RE within 30 days. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard.
Electric Reliability Council of Texas, Inc.		ERCOT agrees with the ISO/RTO SCR comments. However, in addition to the SRC comments, ERCOT offers the following:ERCOT supports future phases of the P81 project to eliminate/retire reliability standards that do not facilitate BES reliability. ERCOT is reviewing all standards to that end, however, developing a list of additional

Organization	Yes or No	Question 3 Comment
		requirements for retirement will require additional time. The SDT should establish a prospective process that provides adequate time and opportunity for entities to perform a meaningful review of remaining requirements to determine which additional requirements warrant retirement and to develop appropriate criteria, if relevant, that may be incremental to the ones proposed in this SAR, and to develop appropriate retirement justifications based on the relevant retirement criteria.
City of Austin dba Austin Energy		FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. Once an interconnection request is actually made with a transmission owner, the transmission owner performs the FAC-002-1 steady-state, short-circuit, and dynamics studies to determine the new interconnection's impact on reliability. During the negotiation of an interconnection agreement the FAC-001-0 referenced material is agreed on and reduced to writing for purposes of constructing, maintaining and operating the interconnection facilities. Also, during the entire interconnection process, as FAC-002-1 provides for, the parties must coordinate and cooperate during the assessment of the reliability impact of the new interconnection facilities. Thus, FAC-001-0, at best, is a best practice or helpful initial guide to an entity considering interconnecting, but provides little, if any, meaningful value to reliability, especially when compared to the actual benefits to reliability via the FAC-002-1 studies, the execution of a negotiated agreement and the coordination of activities during constriction and operation of the new facilities. Accordingly, FAC-001-0 should be retired, and, if necessary, any requirements that protect reliability should be transferred to FAC-002-1. All INT Standards Criteria B 6, 7 and 9Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Thus, we recommend that the Standards Drafting Team retire the INT Reliability Standards and, as necessary, transfer any requirement that protect

Organization	Yes or No	Question 3 Comment
		reliability to the BAL Reliability Standards. All data collection requirements not included in the Initial Phase, more specifically:CIP-005-3a, -4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4CIP-008-3, -4 R2PRC-018-1 R5Criteria B 1, 2 and 9Statement: These requirements are purely data retention requirements with no functional nexus to reliability and, therefore, best handled via compliance monitoring, RSAW or as a data request during an audit. All reporting out requirements not included in the Initial Phase, more specifically:EOP-002-3 R9.2EOP-004-1 R3 and its subrequirements; R4 and R5FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Criteria B 1, 4 and 9Statement: There is no direct connection between reporting out of information to an entity or Regional Entity and protecting reliability. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards.Annual reviewsCIP-002-3, R3; CIP-002 -4 R3CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Criteria B 1, 2, 3, 7 and 9Statement: The annual review and update requirements are arbitrary, administrative and not aligned with the operation and protection of the Bulk Electric System. These requirements should be retired or modified to align with how the Bulk Electric System is operated and protected. Other requirementsCIP-007-3, -4 R7 Criteria B 1, 2, 3 and 7Statement: The essential elements of the process of disposing or redeploying of Cyber Assets and the associated cyber security are set forth in R7.2 and R7.3. To require “formal methods, processes and procedures” appears to require formal documentation for the sake of documentation, rather than allowing the responsible entity to implement a process that achieves the actions required in R7.2 and R7.3,

Organization	Yes or No	Question 3 Comment
		which may or may not include formal procedures, for example. EOP-004-1 R2Criteria B 7 Statement: The analysis of the BES for system disturbances is covered in PRC-004-2.1a R1. The PRC Requirement R1 calls for the analysis of its transmission Protection System Misoperations. We believe that BES analysis is covered inherently through this PRC standard making EOP-004 R1 redundant to the PRC standard.Another factor is the Version 2 of the EOP-004-2 where the requirement to analyze the BES disturbance is noticeably absent. The focus on the EOP-004 is for the reporting of applicable events that are identified in the PRC-004 standard. There is an event analysis reporting process referenced in the NERC Rules of Procedures (ROPs) that handles this requirement. Therefore, this is a redundant requirement. In February of 2012, NERC deployed its Events Analysis Process - incorporating the learnings from two field trials held over the previous year and a half. It includes all the necessary steps that affected operators must take to analyze and report on events that may impair the reliability of the BES. Most Regional Entities have already updated their reporting procedures to match NERC's. Furthermore, NERC and the Regional Entities already have sufficient authority to order analyses and corrective action plans outside of the Reliability Standards. These are important steps for the development of Lessons Learned and trending analyses, but do not contribute to reliable operations. In fact, the demand for near term reporting - some within one hour of the initiation of the event - interferes with the efforts of front-line personnel to mitigate the issue at handBAL-001-0.1a (all requirements), BAL-004-0 (all requirements), BAL-005-0.1b R11; BAL-006-2 (all requirements)Criteria B 6 and 9Statement: BAL-001 requires a 12 month rolling average of ACE and does not impact reliability and should be eliminated (in favor of BAL-002). Consider augmenting NAESB standard WEQ-005.BAL-004 requirement for time error correction is not important for reliability and should be eliminated. It also duplicates NAESB std WEQ-006.In BAL-005 R11, Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE, is not needed for reliability. Ramp rates have minimal impact on ACE calculations, and are already included in the

Organization	Yes or No	Question 3 Comment
		definition of Interchange Schedule in the NERC Glossary as used in R9. The requirement to use agreed upon ramp rates is commercial in nature and is already covered by NAESB standard WEQ-004-17.BAL-006-2 is an after-the-fact accounting of inadvertent interchange and does not impact reliability and should be eliminated. Consider augmenting NAESB standard WEQ-007.CIP-003-3, -4 R2 and its subrequirementsCriteria B 1 and 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is an employee called a CIP senior manager oversees the plan. CIP-004-3, -4 R2.3 Criteria B 9Statement: Whether the entity has a robust up-to-date, trained-on CIP compliance plan may impact reliability, but not whether there is annual training. CIP-004-3, -4 R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is a seven year update to the PRA. CIP-004-3, -4 R4.1Criteria B 1, 9Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it reviews lists every seven days. CIP-004-3, -4 R4.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it revokes access within 24 hours or 7 days. CIP-005-3a, -4a R2.5 and its subrequirementsCriteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the ESP may impact reliability, but not whether specific information is documented. CIP-007-3, -4 R3.1, R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented within 30 days. Also, whether the entity has a robust up-to-date on CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented. CIP-008-3 R1.4Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether specific information is documented within 30 days or a change. EOP-001-1b, -2bCriteria B 7Statement: Duplicative with the other EOP Standards (e.g., Capacity and Energy emergency of EOP-002, Load Shedding of EOP-003, and System Restoration of EOP-005).EOP-002-3 R1Criteria B 7Statement: Duplicates other

Organization	Yes or No	Question 3 Comment
		requirements such as IRO-001-1 R8 and should be retired or modified to reduce redundancy. EOP-002-3 R9 Criteria B 7Statement: When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources). It duplicates NAESB standard WEQ-008 and should be eliminated.EOP-005-2 R1.2.A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration. Criteria B 1, 3 and 7 Statement: With the implementation of NUC-001-2 R2, there is no longer a need for EOP-005-2 R1.2. Specifically, NUC-001-2 R2 requires Nuclear Plant Interface Requirements (NPIRs) to be included in the agreements for operation and maintenance (including restoration process) for off-site nuclear power:R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements1 that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.Given the off-site power requirements of NUC-001-2 which require comprehensive operational interface protocols (including restoration) between nuclear plants and responsible entities as part of the NPIRs, there is no longer a need for the administrative, documentation-only requirement in EOP-005-2 related to the same subject matter.IRO-002-2 (all requirements)Criteria B 7Statement: Redundant with COM-002-2, R1 COM-001-1.1, R1 and IRO-002-2, R2 and R3IRO-005-3a R10Criteria B 9Statement: Confusing requirement. It was intended to address rare cases where entities were told to operate to different SOLs and IROLs. However, because only the TOP and the RC can see these parameters, the only thing a GOP can do is follow a directive.IRO-014-1 R4Criteria B 9Statement: Requirement 4 (including sub-parts) should be rolled up into R1. and eliminated. Requirement 1 should be modified to require "current operating procedures, processes or plans with all adjacent RCs.IRO-015-1 R2.1Criteria B1 and 9Statement: Whether the procedure, process and plan is

Organization	Yes or No	Question 3 Comment
		robust and up-to-date may impact reliability, not whether there are weekly calls.MOD-001-1 and MOD-008-1 (all requirements)Criteria 6 and 9Statement: Do the ATC / TTC standards belong in NERC or NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? I think NERC should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., and I think these can/should be moved to the NAESB standards.Criteria B 6 and 9Statement: This could be handled as a data request from an RE or other Registered Entities and, therefore, would not need a requirement, as there are too many requirements that warrant an attestation that no request was made.MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard.MOD-028-1 (all requirements); MOD-029-1a (all requirements); MOD-030-2 (all requirements)Criteria B 6 and 9Statements: ATC / TTC standards should belong NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? NERC should focus on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc.PRC-022-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.5Criteria B 7Statement: Whether the responsible entity has robust UVLS misoperation and correction action is redundant with PRC-004-1a, -2a. TOP-001-1a R3 and R7 (and its subrequirements)Criteria B 9Statement: For R3, there are three projects in progress addressing the issuance of directives by the RC, BA and TOP. Also, for R7, all outages information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R8 and R 9Criteria B 6, 7 and 9Statement: “Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency”, duplicates VAR-001 and should be eliminated. “Each Balancing Authority shall plan to meet Interchange Schedules and ramps” duplicates the BAL standards and the NEASB standards and should be eliminated.TOP-002-2b R12Criteria B 6 and 9Statement: ATC / TTC standards should belong to NAESB (i.e., MOD-001, MOD-004, MOD-008,

Organization	Yes or No	Question 3 Comment
		MOD-028 thru 030, and TOP-002-2 R12). NERC should focus on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., These can/should be moved to the NAESB standard.TOP-002-2b R14 and R14.1Criteria B 9Statement: All derating information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R15Criteria B 9Statement: Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations is a "how" requirement that is needed to meet other requirements in the standard. It is also not measureable, and the requirement should be eliminated. All weekly forecasts should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-003-1 R1 and its subrequirements; R2 and R3Criteria B 9Statement: All planned outage information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-005-2a R3Criteria B 9Statement: PSEs are not best positioned to provide reliability information.BAL-005-0.1b R1Criteria B7Statement: Introductory statement; redundant with subrequirements MOD-010-0 R2Criteria B 1, 4 and 9Statement: MOD-012-0 R2 was included in the Joint Trade Associations list of suggested requirements for retirement or modification. MOD-010-0 R2 is nearly identical to MOD-012-0 R2 and should also be considered.PER-001-0.1 R1Criteria B7Statement: The TOP portion of this requirement is redundant with TOP-001-1a R1PRC-018-1 R3 (and all sub requirements)Criteria B2 and 4Statement: This requirement involves data collecting and reporting that does not impact the reliability of the BES; could be part of a data request if necessary
Georgia Transmission Corporation		FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. MOD-016-1.1 and MOD-021-1 (all requirements) Criteria Meets Criteria A and a combination of either or all of B1, B2, B3, B4, B 9Statement: MOD-016 through MOD-021 are about long term load forecasting and reporting of actual and forecast loads. Requirements could be eliminated from the standards and replaced with a data collection process (e.g.,

Organization	Yes or No	Question 3 Comment
		TADS/DADS, etc.). Loads to be used in modeling could be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard. Additionally, MODs-016 through 021 have yet to be classified as Tier 1, 2, or 3; nor have they yet to be identified on NERC's Actively Monitored List.PRC-006-1 (R7, R8, and R14) Criteria: Meets Criteria A and a combination of either or all of B1, B3, B4, B9Statement: Recommend these requirements to be eliminated from the standards and replaced with a data collection and or reporting process (e.g., TADS/DADS, etc.). PRC-023-1 (R3.3) Criteria: Meets Criteria A and a combination of either or all of B1, B4, B9Statement: Recommend these requirements to be eliminated from the standards and replaced with a data reporting process.TOP-001-1a (R4) Criteria: Meets Criteria A and B1Statement: Same requirement as TOP-001-1a (R3) which made the Phase I list, only difference is applicability.
Occidental Power Services, Inc.		If the changes listed in Question 2 are not considered in Phase 1, then they should be considered in subsequent phases of the project.
Illinois Municipal Electric Agency		IRO-010-1a R3
Idaho Power Company		MOD-017-0.1 R1.1, R1.2 Criterion B2MOD-018-0 R1 Criterion B7 (Should be covered by MOD-016)MOD-021-1 R1, R2 Criterion B7 (Should be covered by MOD-016)MOD-021-1 R3 Criterion B4
CPS Energy		No additional comments.
Salt River Project		No additions at this time.
Occidental Energy Ventures Corp.		OEVC agrees with the process that the Trades are using to approach this question, but do not agree with some of their priorities. OEVC has only addressed the Requirements where OEVC has additional comments to what the Trades have provided.In addition, OEVC believes the following requirements can also be

Organization	Yes or No	Question 3 Comment
		removed:a) BAL-005, R1.1 - BA metering is financial in nature. Telemetry is already required for reliability.b) TOP-002, R13 - Generator validations are driven by the regions already.FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: OEVC agrees with the Trade's analysis, but will also point out that once connection requirements are in place, they will rarely change. We believe this would mean a lower priority is in order. All INT Standards Criteria B 6, 7 and 9 Statement: Again, OEVC agrees with the Trades on this. It may even be time to suggest that the functional designation of the PSE go away. They serve a marketing purpose and are blind to reliability indicators. All data collection requirements not included in the Initial PhaseCIP-005-3a, -4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4; R7.3CIP-008-3, -4 R2PRC-018-1 R5Criteria B 1, 2 and 9 Statement: OEVC agrees with the Trades. Most of these are captured in Phase I. These fit in the same category. All reporting out requirements not included in the Initial PhaseCIP-001-2a R3 should be modified to eliminate the word "reporting" (added by OEVC)EOP-002-3 R9.2EOP-004-1 R3 and its sub requirements; R4 and R5 FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-010-0 R2 Similar to MOD-012-0 (added by OEVC)MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2 PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Criteria B 1, 4 and 9 Statement: In addition to the Trade's comments, OEVC believes that NERC has an Events Analysis process, RAPA process, and Section 1600 Data Request process that they can invoke to get this information.Annual reviewsCIP-002-2, -4 R4CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Criteria B 1, 2, 3, 7 and 9 Statement: OEVC agrees with the Trades and add that Compliance teams spend far too much time trying to confirm that a RBAM was reviewed and signed off-on. This serves only to add time and expense - especially when conditions have not changed in the preceding year.

Organization	Yes or No	Question 3 Comment
		Other requirements EOP-004-1 R2 Criteria B 7 Statement: OEVC agrees with the Trades. Again, NERC has an Events Analysis process and RAPA process that they can invoke to require analyses. FAC-002-1 R1OEVC agrees that this requirement and five sub-requirements are unnecessary. First of all, the PUC, the BA, and the TOP are highly involved in the interconnection process. It is not clear what extra value is provided by overlapping oversight from the RE and/or NERC. Second, other standards - the TPLs in particular - are directly referenced in the requirement. Those are enforceable already, there is no need to duplicate them here.FAC-008-1 R1.3.5This requirement is already addressed in Phase I.IRO-001-1.1 R8 OEVC believes the intent is to consolidate RC directives in IRO-001 with TOP directives in TOP-001. Since Phase I addresses TOP-001, this seems to have been already accomplished.IRO-005-3a R10Criteria B 9Statement: OEVC agrees with the Trades. This is one that we propose should be a much higher priority. Since the GOP is already told to follow a directive, this requirement makes no sense. MOD-017-0.1 R1.1 and MOD-018-0 (all requirements) ; MOD-020-1 R1OEVC believes that this is redundant with IRO-010 and the new version of TOP-003 when it takes effect.MOD-019-0.1 R1OEVC believes that this is redundant with IRO-010 and the new version of TOP-003 when it takes effect. TOP-002-2b R2; R15OEVC believes that TOP-002 R15 will be resolved by the release of the new TOP standards.TOP-002-2b R14 and R14.1Criteria B 9Statement: OEVC believes that TOP-002 R14 and R14.1 will be resolved by the release of the new TOP standards.TOP-003-1 R1 and its sub requirements; R2 and R3Criteria B 9Statement: OEVC believes that these items will be resolved by the release of the new TOP standards.TOP-005-2a R3Criteria B 9Statement: OEVC agrees with the Trades on this one. Again, it may even be time to suggest that the functional designation of the PSE go away. TOP-006-2 R1.1, R4, R5, R6; TOP-008-1 R2, R4 OEVC believes that that TOP-006 R1.1 will be resolved by the release of the new TOP standards.
NERC Staff Technical Review		Please see NERC Staff's response to question 2 for Phase I requirements that NERC Staff recommends be reviewed for inclusion in a future phase. NERC Staff may propose additional requirements for a future phase of the P81 project at a later date.

Organization	Yes or No	Question 3 Comment
American Electric Power		Please see the response to Question #2 for additional Reliability Standard requirements that AEP would like to be considered as candidates for retirement on this initial, or subsequent, request for comment.
seattle city light		Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Tampa Electric Company		Tampa Electric suggests that the P81 Drafting Team consider the adoption of concepts from the CIP version 5 criteria for consideration under CIP version 3 and 4. In particular Tampa Electric proposes that draft language for CIP-007 patching will reduce administrative burden for compliance with patching process TFEs under current versions (CIP-007 V3 and V4). The version 5 draft Guidelines and Technical Basis for CIP-007 V5 states: R2.1 A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. R2.2 Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.
Manitoba Hydro		The following statement should be removed from the standard as it does not support reliability of the BES [B8]:FAC-013-2 R5. 'However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request'The following statement should be removed from the standard as it does not support reliability or provide any protection to the BES. [B8]:FAC-013-2 R6. 'If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to

Organization	Yes or No	Question 3 Comment
		that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information'.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade Associations).		The Trade Associations support the following list of Reliability Standard requirements to be retired or modified in a subsequent phase of the P81 project. To assist the Standards Drafting Team decide what should be considered in phase 2, phase 3 etc., the Trade Associations have listed the requirements in the order of importance - with those at the top of the list candidates for phase 2. The Trade Associations understand, however, that the decision on how best to proceed with phase 2, phase 3 will be weighed by the Standards Drafting Team, and, therefore, have not indicated any bright line on what should or should not be included in phase 2 versus phase 3, etc. The Trade Associations further note that the list of requirements listed below may be supplemented with additional requirements as the phase 2/phase 3 discussions evolve. Additionally, the Trade Associations believe that additional criteria for elimination may be proposed as part of the phase 2/phase 3 process.FAC-001-0 (all requirements)Criteria B 1, 3 and 6Statement: The requirement in FAC-001-0 to document and publish facility connection requirements has no impact on reliability. It is purely a document that those considering to interconnect with a transmission entity may review as a reference. Once an interconnection request is actually submitted to a transmission owner, the transmission owner performs the FAC-002-1 steady-state, short-circuit, and dynamics studies to determine the new interconnection's impact on reliability. During the negotiation of an interconnection agreement the FAC-001-0 reference material is agreed on and reduced to writing for purposes of constructing, maintaining and operating the interconnection facilities. Also, FAC-002-1 imposes an obligation on the parties to coordinate and cooperate during the assessment of the reliability impact of the new interconnection facilities. Thus, FAC-001-0, at best, is a best practice or helpful initial guide to an entity considering interconnecting, but provides little, if any, meaningful value to reliability, especially when compared to the actual benefits to reliability via the FAC-002-1

Organization	Yes or No	Question 3 Comment
		studies, the execution of a negotiated agreement and the coordination of activities during construction and operation of the new facilities. Accordingly, FAC-001-0 should be retired, and, if necessary, the transfer of any requirements that protect reliability to FAC-002-1. All INT Standards (With the exception of INT-007-1 R1.2 which is part of and should remain in the Initial Phase.)Criteria B 6, 7 and 9 Statement: Many of the INT Reliability Standard requirements are very close to duplicative of similar requirements in the BAL Reliability Standards or address commercial matters. As drafted, the INT Reliability Standards include tasks or activities that do little, if anything, to promote the protection the Bulk Electric System. Thus, it is recommended that the Standards Drafting Team retire the INT Reliability Standards, and, as necessary, transfer any requirement that protect reliability to the BAL Reliability Standards. ALL DATA COLLECTION REQUIREMENTS NOT INCLUDED IN THE INITIAL PHASECIP-005-3a, -4a R5.3CIP-006-3c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4CIP-008-3, -4 R2PRC-018-1 R5Criteria B 1, 2 and 9Statement: These requirements are purely a data retention requirement with no functional nexus to reliability, and, therefore, are best handled via compliance monitoring, RSAWs or as a data request during an audit.ALL REPORTING OUT REQUIREMENTS NOT INCLUDED IN THE INITIAL PHASEEOP-002-3 R9.2EOP-004-1 R3 and its subrequirements; R4 and R5FAC-003-1 R3; FAC-003-1 R3.1: FAC-003-1 R3.2: FAC-003-1 R3.3: FAC-003-1 R3.4: FAC-003-1 R3.4.1: FAC-003-1 R3.4.2: FAC-003-1 R3.4.3: FAC-003-1 R4FAC-010-2.1 R5FAC-011-2 R5FAC-013-2 R6MOD-012-0 R2MOD-020-0 R1MOD-021-1 R3PRC-004-1a R3: PRC-004-2a R3: PRC-004-WECC-1 R.3.PRC-007-0 R2; PRC-007-0 R3; PRC-009-0 R2; PRC-011-0 R2; PRC-015-0 R3; PRC-016-0.1 R3; PRC-017-0 R2; PRC-021-1 R2TPL-001-0.1 R3; TPL-002-0b R3; TPL-003-0a R3; TPL-004-0 R2.Criteria B 1, 4 and 9Statement: There is no direct nexus between reporting out of information to an entity or Regional Entity and protecting reliability. If the Regional Entity desires to review information for purposes of monitoring reliability or assessing risk, the information should be collected via vehicles other than the Reliability Standards.Annual reviewsCIP-002-3, R3; CIP-002 -4 R3CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4 R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4

Organization	Yes or No	Question 3 Comment
		R9CIP-009-3, -4 R1EOP-005-1 R1; EOP-005-2 R3.1EOP-008-0 R1.7EOP-008-1 R5IRO-014-1 R4.3Criteria B 1, 2, 3, 7 and 9Statement: The annual review and update requirements are arbitrary, administrative and not aligned with the operation and protection of the Bulk Electric System. These requirements should be retired or modified to align with how the Bulk Electric System is operated and protected. OTHER REQUIREMENTSCIP-007-3, -4 R7 Criteria B 1, 2, 3 and 7Statement: The essential elements of the process of disposing or redeploying of Cyber Assets and the associated cyber security are set forth in R7.2 and R7.3. To require "formal methods, processes and procedures" appears to require formal documentation for the sake of documentation, rather than allowing the responsible entity to implement a process that achieves the actions required in R7.2 and R7.3, which may or may not include formal procedures, for example. EOP-004-1 R2Criteria B 7 Statement: The analysis of the BES for system disturbances is covered in the PRC-004-2.1a R1. The PRC Requirement R1 calls for the analysis of its transmission Protection System Misoperations. We believe that BES analysis is covered inherently through this PRC standard, making EOP-004 R1 redundant to the PRC standard. Another factor that was considered is the notable absence of any requirement in EOP-004-2 to analyze the BES disturbance. The focus of EOP-004 is on the reporting of applicable events that are identified in the PRC-004 standard. There is an event analysis reporting process referenced in the NERC Rules of Procedures (ROP) that addresses this requirement. Therefore, this is a redundant requirement. In February of 2012, NERC deployed its Events Analysis Process - incorporating the learnings from two field trials held over the previous year and a half. It includes all the necessary steps that affected operators must take to analyze and report on events that may impair the reliability of the BES. Most Regional Entities have already updated their reporting procedures to match NERC's. Furthermore, NERC and the Regional Entities already have sufficient authority to order analyses and corrective action plans outside of the Reliability Standards. These are important steps for the development of Lessons Learned and trending analyses, but do not contribute to reliable operations. In fact, it is arguable that the demand for near term reporting - some within one hour of the

Organization	Yes or No	Question 3 Comment
		initiation of the event - interferes with the efforts of front-line personnel to mitigate the issue at hand BAL-004-0 (all requirements), BAL-005-0.1b R11; BAL-006-2 (all requirements)Criteria B 6 and 9Statement: BAL-004 requirement for time error correction is not important for reliability and should be eliminated. BAL-004 also duplicates NAESB standard WEQ-006.BAL-005 R11 states that Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE. This requirement is not needed for reliability. Ramp rates have minimal impact on ACE calculations, and are already included in the definition of Interchange Schedule in the NERC Glossary as used in R9. The requirement to use agreed upon ramp rates is commercial in nature and is already covered by NAESB standard WEQ-004-17.BAL-006-2 is an after the fact accounting of inadvertent interchange and does not impact reliability and should be eliminated. Consider augmenting NAESB standard WEQ-007. CIP-003-3, -4 R2 and its subrequirementsCriteria B 1 and 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is an employee called a CIP senior manager that oversees the plan. CIP-004-3, -4 R2.3 Criteria B 9Statement: Whether the entity has a robust up-to-date, trained-on CIP compliance plan may impact reliability, but not whether there is annual training. CIP-004-3, -4 R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether there is a seven year update to the personnel risk assessment(PRA). CIP-004-3, -4 R4.1Criteria B 1, 9Statement: Whether the entity has a robust up-to-date on CIP compliance plan may impact reliability, but not whether it reviews lists every seven days. CIP-005-3a, -4a R2.5 and its subrequirementsCriteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the ESP may impact reliability, but not whether specific information is documented. CIP-007-3, -4 R3.1, R3.2Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but not whether specific information is documented within 30 days. Also, whether the entity has a robust up-to-date CIP compliance plan to protect the PSP may impact reliability, but

Organization	Yes or No	Question 3 Comment
		not whether specific information is documented. CIP-008-3 R1.4Criteria B 1, 9Statement: Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether specific information is documented within 30 days or a change. EOP-001-1b, -2bCriteria B 7Statement: Duplicative with the other EOP Standards (e.g., Capacity and Energy emergency of EOP-002, Load Shedding of EOP-003, and System Restoration of EOP-005).EOP-002-3 R1Criteria B 7Statement: Duplicative of other requirements such as IRO-001-1 R8, and should be retired or modified to reduce redundancy. EOP-002-3 R9 Criteria B 7Statement: When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources). It is duplicative of NAESB standard WEQ-008 and should be eliminated.EOP-005-2 R1.2.A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration. Criteria B 1, 3 and 7 Statement: With the implementation of NUC-001-2 R2, there is no longer a need for EOP-005-2 R1.2. Specifically, NUC-001-2 R2 requires Nuclear Plant Interface Requirements (NPIRs) to be included in the agreements for operation and maintenance (including restoration process) for off-site nuclear power:Ref: NUC-001-2 R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements1 that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.Given the off-site power requirements of NUC-001-2 which require comprehensive operational interface protocols (including restoration) between nuclear plants and responsible entities as part of the NPIRs, there is no longer a need for the administrative, documentation-only requirement in EOP-005-2 related to the same subject matter.FAC-013-1 (all requirements)Criteria B 6Statement: It is really a commercial planning practice suitable for Order 1000 under Section 205/206 as opposed to Section 215.IRO-002-2 (all requirements)Criteria B

Organization	Yes or No	Question 3 Comment
		7Statement: Redundant with COM-002-2, R1 COM-001-1.1, R1 and IRO-002-2, R2 and R3IRO-005-3a R10Criteria B 9Statement: Confusing requirement. It was intended to address rare cases where entities were told to operate to different SOLs and IROLs. However, since only the TOP and the RC can see these parameters, the only thing a GOP can do is follow a directive.IRO-014-1 R4Criteria B 9Statement: Requirement 4 (including sub-parts) should be rolled up into R1 and eliminated. Requirement 1 should be modified to require "current operating procedures, processes or plans with all adjacent RCs.IRO-015-1 R2.1Criteria B1 and 9Statement: Whether the procedure, process and plan is robust and up-to-date may impact reliability, not whether there are weekly calls. MOD-001-1 and MOD-008-1 (all requirements)Criteria B 6 and 9Statement: NERC should be focused on modeling the BES and managing SOLs and IROLs, the methodologies for the determination of CBM, TTC and ATC are commercial matters associated with the reservation and allocation of rights to transfer capability among transmission customers. While transfer capability calculations should be based on models of the BES, the NAESB WEQ should address the issues raised in MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12.Criteria B 6 and 9Statement: This could be handled as a data request from an RE or other Registered Entities, and therefore would not need a requirement, as there are too many requirements that warrant an attestation that no request was made.MOD-016-1.1 and MOD-021-1 (all requirements) Criteria B 9Statement: MOD-016 through MOD-021 are all about long term load forecasting and reporting of actual loads. Most of this can be eliminated from the standards and replaced with a data collection process (e.g., DADS). Loads to be used in modeling should be incorporated in the data requirements of MOD-010 and MOD-012 and not a separate standard.MOD-019-0.1 R1Criteria B 1, 2, and 9Statement: MOD-019-0.1 covers “Reporting of Interruptible Demands and Direct Control Load Management,” which requires reporting of a forecast of interruptible demand and direct control load management data. This reporting is administrative in nature, and the information is not important for reliability. The data is best gathered through DADS and not through a standard.MOD-028-1 (all requirements); MOD-029-1a (all requirements);

Organization	Yes or No	Question 3 Comment
		MOD-030-2 (all requirements)Criteria B 6 and 9Statement: Do the ATC / TTC standards belong in NERC or NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? I think NERC should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc., and I think these can/should be moved to the NAESB standards. PRC-011-0 R1 Criteria B 4 and 9Statement: Requirements for maintenance of under-frequency load shedding systems ("UFLS") and under-voltage load shedding systems ("UVLS") are not needed to meet an adequate level of BES reliability. UFLS and UVLS installations are widely distributed. Distribution circuit outages, distribution field switching, and varying load profiles, such as peak and off-peak, could impact the amount of load that would be automatically shed by UFLS and UVLS. Therefore, entities must include adequate margins above their obligation to be able to meet the obligated load shed at all times as required by Reliability Standards, such as PRC-006 and PRC-007, that are performance-based, or results-based. While UFLS and UVLS are, of course, important safety-net systems, PRC-011-0 R 1 maintenance requirement is not needed to provide a "defense-in-depth" approach due to the margins required to meet performance-based requirements. Thus, Like PRC-008-0 R1 included in Phase I, Reliability Standard PRC-011-0 R1 which involves maintenance of UVLS, is not needed. In fact, it is typically the same relays and associated equipment that provides both the UFLS and the UVLS functions. PRC-022-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.5Criteria B 7Statement: Whether the responsible entity has robust UVLS misoperation and correction action is redundant with PRC-004-1a, -2a. TOP-001-1a R7 (and its subrequirements)Criteria B 9Statement: For R3, there are three projects in progress addressing the issuance of directives by the RC, BA, and TOP. This includes COM-003-1's requirements for the issuances of "not quite directives" Also, for R7 All outages information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R8 and R 9Criteria B 6, 7 and 9Statement: "Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency", is duplicative of VAR-001 (and incorrect) and should be eliminated. "Each Balancing Authority shall plan to meet Interchange Schedules and ramps", is duplicative of the

Organization	Yes or No	Question 3 Comment
		BAL standards and the NAESB standards and should be eliminated.TOP-002-2b R12Criteria B 6 and 9Statement: The ATC / TTC standards may belong in NAESB (i.e., MOD-001, MOD-004, MOD-008, MOD-028 thru 030, and TOP-002-2 R12)? NERC standards should be focused on managing SOLs and IROLs, whereas NAESB on TTC, ATC, etc.TOP-002-2b R14 and R14.1Criteria B 9Statement: All derating information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-002-2b R15Criteria B 9Statement: Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations is a "how" requirement that is needed to meet other requirements in the standard. It is also not measureable, and the requirement should be eliminated. All weekly forecasts should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-003-1 R1 and its subrequirements; R2 and R3Criteria B 9Statement: All planned outage information should be submitted to the TOP and/or BA in accordance with their data requirements.TOP-005-2a R3Criteria B 9Statement: PSEs are not best positioned to provide reliability information.
SPP Standards Review Group		VAR-002 R3 Status changes on AVRs - Quite often status changes to AVRs may be made for only a matter of seconds. These changes do not impact the reliability of the BES but still require a call be made for notification of the change. Perhaps the requirement could be changed such that only status changes which impact the BES need to be reported. This hits on Items 4, 5, 8 and 9 in Criterion B.FAC-003-1 R1.3 - Specific training is required for personnel involved with vegetation management programs. This requirement is purely administrative (Criterion B.1) and does not, in and of itself, benefit the reliability of the BES. (Although this requirement has been removed in subsequent versions of this standard (FAC-003-2 and FAC-003-3), it remains in effect today. It needs to be retired.)While we don't have an extensive list at this time, we would hope that the drafting team will ask for potential candidates which fit this category at some point in the future prior to the start of work on the latter phases of the project.

Organization	Yes or No	Question 3 Comment
Ameren		We support and agree with Trade Association's comments and their suggested list of Reliability Standard requirements to be retired or modified in the subsequent phase of the P81 Project. In addition, we suggest that IRO-005-3, R10 should be modify to eliminate its applicability to LSE and PSE in addition to GOP. While the IRO-005-3_1a, R10 is necessary for the reliable operation of the BES, its applicability to LSE and PSE also is questionable as these entities do not "operate" the BES. We believe that it is redundant (criteria B7) with other requirements where these entities (GOP, LSE, and PSE) have to follow the RC and/or TOP directives.
Wolverine Power Supply Cooperative, Inc.		Wolverine agrees with the list of requirements that the trade associations are submitting. We are a member of NRECA and agree with their comments.

4. If you have any other comments or suggestions on the draft SAR that you have not already provided in response to the previous questions, please provide them here.

Summary Consideration:

Comment

NERC staff requests that the scope of the SAR include currently-pending versions of related Reliability Standards to address requirements proposed in Phase I that are also included in a subsequent version of the standard that has been adopted by the NERC Board of Trustees, but not yet approved by FERC. Manitoba Hydro has a similar concern. NERC staff also requests that technical justifications only rely on Commission-approved Reliability Standards and how removal of a requirement will "increase in efficiency of the ERO compliance program" consistent with the language of P81.

Response

The P81 SDT added a footnote to the SAR to address how pending versions of related Reliability Standards (i.e., NERC BOT adopted) are considered so that eliminated requirements carry through to any new NERC BOT adopted versions. In addition, the P81 SDT is developing a technical white paper that it believes will provide a sound, technical basis for removal of each NERC Reliability Standard requirement proposed in Phase I. As appropriate, the technical basis will only reference or rely on Commission-approved Reliability Standards. The technical white paper being developed by the P81 SDT will generally address the issue of efficiency gains in the ERO compliance program with a blanket statement, on a requirement basis, or a combination of both.

Comment

Kansas City Power & Light states that the retirement of the requirements should not have a ripple impact in other standards or requirements.

Response

Although it is unclear to the P81 SDT what is meant by the term "ripple impact," it is believed to be similar to Criterion C's defense in depth concept. In the future, it would be helpful to provide some examples where the removal of a NERC Reliability Standard requirement may have a ripple impact in other standards. At this time, the P81 SDT believes the consideration of Criterion C (specifically, the consideration of whether retiring a requirement will have any negative impact on the defense-in-depth protection of the BES) ensures that other standards and requirements are not negatively impacted.

Comment

Entergy Services, Inc. states that during future phases industry input should be gathered in a more formal process. PPL Corporation NERC Registered Affiliates had a similar suggestion to increase stakeholder involvement.

Response

The P81 SDT is using the approved Standard Process Manual (SPM) for Phase I, and, at this point, plans to use the SPM in effect at the time for future phases of this project as well. The SDT acknowledges that stakeholder input may need to be gathered in a manner differently in subsequent phases than that used for Phase I, as subsequent phases may be more involved than simply removing requirements in their entirety and will likely require combining and/or re-wording of existing requirements.

Comment

Dominion observed some highlighting and number issues in the draft documents and appears to suggest we add IRO-001-1a R8.

Response

Requirement 8 of NERC Reliability Standard IRO-001-1a, while redundant to TOP-001-1a R3 with regard to Reliability Coordinators, will need to remain to ensure that a NERC Reliability Standard exists that addresses the need for entities to comply with a Reliability Coordinator's Reliability Directives.

Typographical errors will be addressed by the SDT.

The spreadsheet with proposed retirements on the NERC website will be manually sorted to ensure appropriate ordering of requirements on future revisions.

Comment

South Carolina Electric and Gas states that instead of retiring R2 of EOP-009-0 could the whole standard can be replaced by the new EOP-005?

Response

Yes, it is the SDT's understanding that NERC Reliability Standard EOP-009-0 will be retired when Standard EOP-005-2 becomes enforceable (July 1, 2013).

Comment

Idaho Power Company, among other things, suggests the combing of MOD standards 016 through 021.

Response

The suggested combining of NERC Reliability Standards MOD-016 through MOD-021 has been referred to the Question 3 sub-team for consideration for Phase II.

Comment

ACES Power Marketing Standards Collaborators and Electric Reliability Council of Texas, Inc. state that NERC needs to develop guidance that includes these criteria for drafting teams to avoid developing requirements that offer little reliability value in the future.

Response

The P81 SDT agrees that NERC-developed guidance is needed for standard drafting teams to ensure that new requirements consider the criteria established by the P81 SDT. The P81 SDT will address this issue with the NERC Standards Committee.

Comment

Georgia System Operations Corporation and Georgia Transmission Corporation suggest the consideration of requirements for retirement that supports NERC programs other than the mandatory Reliability Standards.

Response

The SDT appreciates the comments. The SDT believes that the criteria, as drafted, should capture those requirements that Georgia System Operations Corporation and Georgia Transmission Corporation are concerned about.

Organization	Yes or No	Question 4 Comment
NERC Staff Technical Review		(1) NERC Staff notes that the scope of the SAR should be expanded to include currently-pending versions of related Reliability Standards to address requirements proposed in Phase I that are also included in a subsequent version of the standard that has been adopted by the NERC Board of Trustees, but not yet approved by FERC. NERC Staff suggests that footnotes could be included to capture these situations.(2) NERC Staff submits that the technical justification for removal of particular requirements should not be a restatement of the Criteria (see e.g., INT-007-1 R1.2). Nor should the technical justifications reference and/or rely upon for support any Reliability Standards unless those Reliability Standards are Commission-approved. (3) NERC Staff suggests that the technical justifications for the satisfaction of the Criteria

Organization	Yes or No	Question 4 Comment
		should include an explanation of how removal of the requirement will result in an "increase in efficiency of the ERO compliance program" consistent with the language of P81.
Duke Energy		Duke Energy generally supports the comments submitted by The Edison Electric Institute (EEI) and the process being used to respond to the Commission's invitation in the FFT Order.
Kansas City Power & Light		Efforts need to be made to make sure that the retirement of the requirements listed in "Proposed Requirements for Retirement in Phase 1 of Project 2013-02: Paragraph 81" don't have a ripple impact in other standards or requirements.
Entergy Services, Inc.		For future phases, indutry input should be gathered in a more formal process to allow for suggestions for re-wording or suggesting additional requirements for removal.
Tucson Electric Power		I appreciate the fact that there is a review of the NERC Standards as well as a review of the absolute need for various Standards and/or requirements. I also appreciate that the regulatory bodies are agreeable to such changes and improvements to the compliance process.
Illinois Municipal Electric Agency		Illinois Municipal Electric Agency fully supports this initiative by the collaboration group which suppports NERC's application of a risk-based focus to it's programs, and which is consistent with SPIG Recommendation 4.
Dominion		In the Complete Set of Standards with Proposed Retirements for Phase 1 pdf; Need to add IRO-001-1a R8 and MOD-004-1 R8 needs to be completely highlighted. In the Spreadsheet with Proposed Retirements; Suggest the MOD-004-1 Requirements be put in numeric order. Need to add IRO-001-1a R8; it is not listed on the spreadsheet.
South Carolina Electric and Gas		Instead of retiring R2 of EOP-009-0 could the whole standard can be replaced by the new EOP-005?

Organization	Yes or No	Question 4 Comment
Manitoba Hydro		It is not clear what will happen in instances where this project proposes to remove a requirement from a FERC approved Reliability Standard when the NERC BOT has already approved a newer version of that same standard. Will the newer BOT approved version also be modified if it includes one of the requirements in question? What if industry has already resolved one of these issues in the next version of a standard? Shouldn't we just implement the newer version?
MidAmerican Energy Company		MidAmerican Energy Company supports the draft SAR as a positive step to allow Responsible Entities, Regional Entities, NERC and FERC to focus their combined efforts on protecting the Bulk Electric System.
Idaho Power Company		MOD standards 016 through 021 should be combined into a single standard, removing duplication and retiring requirements which are "reporting-only" and/or have little discernable reliability benefit.We agree with the stated Purpose or Goal of the proposed standard of setting forth specific Reliability Standard requirement evaluation criteria and establishing a multi-phased process for addressing these Reliability Standard requirements. We agree with and support this Reliability Standard requirement evaluation and proposed multi-phased process based on the following:We believe there is value in differentiation of violations based on risk. We believe that not all violations pose the same risk to reliability, so they should not all be treated the same. Focusing on the greatest risks to reliability will allow for more efficient use of resources while improving the reliability of the BES through an application of structured risk management.
ACES Power Marketing Standards Collaborators		NERC needs to develop guidance that includes these criteria for drafting teams to avoid developing requirements that offer little reliability value in the future. There are many standards currently being developed that include similar kinds of requirements that will make a future exercise like this necessary. NERC should expend every effort to avoid such a future situation. Some examples can be found in Project 2007-09 Generator Verification. Proposed MOD-027-1 R3 through R5 largely

Organization	Yes or No	Question 4 Comment
		memorializes the administrative interactions that must occur between the GO and TP to develop a good active power/frequency control model. PRC-004-3 Part 4.2 in Project 2010-05.1 Misoperations is another example. It requires maintenance of data regarding Corrective Action Plans. These are administrative requirements and are unnecessary.
CPS Energy		No additional comments.
Independent Electricity System Operator		No comments.
Occidental Energy Ventures Corp.		OEVC Agrees with the Trade Associations on this response.
Pepco Holdings Inc & Affiliates		Pepco Holdings Inc supports this project. Additionallyl Pepco Holdings Inc supports the comments provided by EEI.
Georgia System Operations Corporation		Reliability Standard requirements are those that provide for Reliable Operation, including without limiting the foregoing, requirements for the operation of existing Facilities, including cyber security protection, and including the design of planned additions or modifications to such Facilities to the extent necessary for Reliable Operation. NERC administers other programs, such as industry alerts, reliability assessments, event and trend analyses, education, and monitoring and enforcing Reliability Standards. These other programs are designed to work in concert with Reliability Standards to support reliable operation. NERC requirements relating to administering these other programs are very important but are not Reliability Standard requirements.One of the criteria for evaluating the elimination of a Reliability Standard requirement is that it is purely reporting. There are a number of NERC requirements for these other NERC programs embedded in Reliability Standards. Most of them are purely reporting. However, to the extent that there may be other requirements for these NERC programs embedded that are not purely

Organization	Yes or No	Question 4 Comment
		reporting, they should also be considered for elimination. Reliability Standards by definition are not mechanisms for the administration of those other NERC programs.
Georgia Transmission Corporation		Reliability Standard requirements are those that provide for Reliable Operation, including without limiting the foregoing, requirements for the operation of existing Facilities, including cyber security protection, and including the design of planned additions or modifications to such Facilities to the extent necessary for Reliable Operation. NERC administers other programs, such as industry alerts, reliability assessments, event and trend analyses, education, and monitoring and enforcing Reliability Standards. These other programs are designed to work in concert with Reliability Standards to support reliable operation. NERC requirements relating to administering these other programs are very important but are not Reliability Standard requirements.One of the criteria for evaluating the elimination of a Reliability Standard requirement is that it is purely reporting. There are a number of NERC requirements for these other NERC programs embedded in Reliability Standards. Most of them are purely reporting. However, to the extent that there may be other requirements for these NERC programs embedded that are not purely reporting, they should also be considered for elimination. Reliability Standards by definition are not mechanisms for the administration of those other NERC programs. GTC recommends identifying these requirements (ex. MOD-016 through 021) and appending them to the Phase I list.
seattle city light		Seattle City Light supports the consolidated comments of the industry Trade Organizations.
Tampa Electric Company		Tampa Electric recommends that the P81 DT ensure that the CIP requirements proposed for removal via P81 are also removed from v5 of the NERC CIP standards. Tampa Electric also supports the consideration of the following for NERC CIP standards: Removal of data collection requirements: CIP-005-3a, -4a R5.3CIP-006c, -4c R7, R8.3CIP-007-3, -4 R5.1.2; R6.4; R7.3CIP-008-3, -4 R2Removal of annual review requirements: CIP-002-2, -4 R4CIP-003-3, -4 R1.3; CIP-003-3, -4 R4.3; CIP-003-3, - 4

Organization	Yes or No	Question 4 Comment
		R5.1.2; CIP-003-3, - 4 R5.3CIP-006-3c, -4 R1.8CIP-007-3, -4 R9CIP-009-3, -4 R1
Transmission Agency of Northern California		TANC commends FERC for soliciting input on ways to eliminate requirements that are redundant or provide little protection for the bulk power system. TANC believes that NERC has proposed an appropriate response to this opportunity and looks forward to further initiatives that prioritize reliability ahead of compliance.
SERC EC Planning Standards Subcommittee		The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers.
SPP Standards Review Group		The following are typos we found in the SAR:Either delete the 'an' or make 'processes' singular in Technical Criteria B.2.(b).Either delete the 'that' in the 5th line or the 'to' in the 6th line of the Statement paragraph under CIP-001-2a R4. This is the 3rd sentence in the paragraph.Insert an 'a' between 'require' and 'new' in the last sentence of the Statement paragraph under CIP-003-3, -4 R4.2.
City of Austin dba Austin Energy		The P81 project should be considered a high priority Standards development project for the following reasons:(1) Responsive to P81 of FERC's March 15, 2012 order and SPIG Recommendation No. 4(2) Will increase efficiency of the ERO compliance programs(3) Requirements submitted for the initial phase appear to be clear candidates on their face and should not require extensive technical research(4) The collaborative nature of the project is an example for future work, because it advances the project while reducing the impact on stakeholders and NERC staff(5) The proposed pace of the project sets an example for future work (6) Furthers the focus on results, performance based Reliability Standards (7) May provide a roadmap of what should or should not be a requirement in future Reliability Standards(8) The draft P81 SAR criteria is designed to be sufficiently broad to capture all FERC approved reliability Standards that are unnecessary, redundant or do little to protect reliability (9) To eliminate Reliability Standards requirements that deter from our

Organization	Yes or No	Question 4 Comment
		focus on reliability Based on these benefits, we support the Standards Drafting Team and NERC staff working together to file the initial list of Reliability Standards for retirement with the Federal Energy Regulatory Commission prior to the end of the year and that the Standards Drafting Team also make significant progress on the scope of the phase two P81 Reliability Standards list by the end of the year.
PPL Corporation NERC Registered Affiliates		The PPL Companies generally support the concept and process being recommended, but are concerned that the stakeholder involvement in the process may be lacking. During the webinar on August 21, 2012 the drafting team members stated that the Standards Development Process will be utilized for all Phases of the project. However, the SAR does not indicate that the SDP is mandated. The Companies recommend that the entire SAR specifically state the the Standards Development Process will be used where the SDT must respond to comments and a stakeholder vote for approval. Additionally, the process should allow for individual (or groups) of stakeholders to request a standard's removal or modification that is not designated by the SDT for removal.
The Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the Electric Power Supply Association (EPSA), the Transmission Access Policy Study Group (TAPS), Electricity Consumers Resource Council (ELCON), the American Public Power Association (APPA), the Large Public Power Council (LPPC) and, the Canadian Electricity Association (CEA) (collectively, the Trade		The Trade Associations believe that the P81 project should be considered a high priority Standards development project for the following reasons: o Responsive to P81 of FERC's March 15, 2012 order and SPIG Recommendation No. 4 o Will increase efficiency of the ERO compliance programs o Requirements submitted for the initial phase appear to be clear candidates on their face and should not require extensive technical research o The collaborative nature of the project is an example for future work, because it advances the project while reducing the impact on stakeholders and NERC staff o The proposed pace of the project sets an example for future work o Furthers the focus on results, performance based Reliability Standards o May provide a roadmap of what should or should not be a requirement in future Reliability Standards o The draft P81 SAR criteria are designed to be sufficiently broad to capture all FERC approved reliability Standards that are unnecessary, redundant or do little to protect reliability o Eliminating Reliability Standards requirements that are unnecessary, redundant or do little to protect reliability will

Organization	Yes or No	Question 4 Comment
Associations).		eliminate distractions from our focus on reliability Based on these benefits, the Trade Associations strongly support the Standards Drafting Team and NERC staff working together to file the initial list of Reliability Standards for retirement with the Federal Energy Regulatory Commission prior to the end of the year, and that the Standards Drafting Team also make significant progress on the scope of the phase two P81 Reliability Standards list by the end of the year.
City of Garland		This is a good start on removing requirements that are either redundant or provide little / no protection for Bulk-Power System reliability.
Electric Reliability Council of Texas, Inc.		This SAR offers significant potential value by retiring requirements that provide no BES reliability value, but nonetheless require commitment of time and resources for both regulated entities and regulators to effect and oversee compliance, respectively, and also pose liability risk for no reason, given that they provide no reliability value. However, the substance of the requirements (e.g. administrative processes, etc.) may have non-essential value unrelated to system reliability. To the extent the SDT/industry/NERC believe there may be some non-mandatory use for this information outside of the reliability standards, the information could be considered for guidance in another format, such as guidelines, best practice documentation or lessons learned. If such an effort is deemed worthwhile, it should be established in a separate process/effort, and should not distract from moving this and future phases of this SAR forward in the most efficient and effective manner to achieve the significant benefits that may result from this SAR. In addition, the standards process going forward should include consideration of whether a proposed standard addresses a reliability requirement, is cost effective and meets the reliability-based standards criteria of “what” needs to be met and not “how” an entity will meet the standard which is better address through guidelines, best practices and/or lessons learned.
Central Husdon Gas & Electric		We agree with the criteria as listed, however, we believe that another criterion must be added. This criterion is that the retirement of a requirement must not create a

Organization	Yes or No	Question 4 Comment
Corporation		compliance gap for Entities. Several of the NERC requirements have been crafted to afford Entities a means to display compliance. Retirement of these requirements can place an Entity's compliance efforts in jeopardy. A salient example of this is identified below:Central Hudson Gas & Electric Corporation strongly disagrees with the inclusion of CIP-003-3, -4 Requirements R3, R3.1, R3.2, R3.3 as candidates for retirement. The reasons stated in the SAR in favor of inclusion are that these requirements are administrative in nature and are purely examples of a documentation process. Further it is stated in the SAR that they, ".... have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements." This last statement is precisely the reason why the aforementioned requirements were included in the standard. These requirements allow Registered Entities to, on rare occasions, take an exception to one or several of the CIP requirements (for a limited period of time) if they (1) have valid cause (major emergency, Force Majeure, etc.), (2) document the occurrence and (3) are reviewed and approved by the CIP Senior Manager. This process supports the Registered Entity's compliance effort and acknowledges the need for special protocols to address emergency circumstances. Without such a process, the only recourse for the Registered Entity is to self-report a violation which is not within its control. In other words, retirement of these requirements would force the Registered Entity to be in full compliance with ALL CIP Standards ALL the time regardless of circumstance. The concept of 'realistic expectation' was undoubtedly the reason these requirements were crafted and included in the standard. Further, with regard to the Registered Entity's decision to claim an exception, a system of checks and balances already exists. At the time of a compliance audit of the standard's requirements, the Regional Entity reviews and makes a determination as to whether the actions taken by the Registered Entity were warranted.
NV Energy		We commend NERC and the Drafting Team on their efforts thus far in this important initiative. This process will serve to better focus the industry's limited resources on

Organization	Yes or No	Question 4 Comment
		activities that are necessary for reliability.
SRC		We support the P81 team's efforts and appreciate the effort to pull together this initial list of criteria and requirements. The SRC is looking forward to seeing a concrete timeline for the project.
Western Electricity Coordinating Council		WECC recognizes and appreciates the large amount of work done in a short time on this project and appreciates the opportunity to proved our comments.
American Electric Power		While AEP supports the efforts of this drafting team, it might have been advantageous to first agree on the criteria as a first phase, and then once determined, enter a second phase where requirements were proposed based upon the agreed-upon criteria. This might enable the fast-tracking of the criteria to be used by other concurrent projects and project teams.

END OF REPORT

A. Introduction

1. **Title:** **Automatic Generation Control**

2. **Number:** BAL-005-0.2b

3. **Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.

4. **Applicability:**

   4.1. Balancing Authorities

   4.2. Generator Operators

   4.3. Transmission Operators

   4.4. Load Serving Entities

5. **Effective Date:** May 13, 2009

B. Requirements

R1. All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.

R1.1. Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.

R1.2. Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.

R1.3. Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retired)

R3. A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.

R4. A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.

R5. A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.

R6. The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

R7. The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.

R8. The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.

R8.1. Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.

R9. The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.

R9.1. Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.

R10. The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.

R11. Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.

R12. Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.

R12.1. Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.

R12.2. Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.

R12.3. Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.

R13. Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.

R14. The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.

R15. The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

R16. The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

1.1.1. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.

1.1.2. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

1.3.1. Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.

1.3.2. Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Effective Date: August 27, 2008 (U.S.)

Interpretation of BAL-005-0 Automatic Generation Control, R17

Request for Clarification received from PGE on July 31, 2007

PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

BAL-005-0

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25% of full scale
Remote terminal unit	≤ 0.25% of full scale
Potential transformer	≤ 0.30% of full scale
Current transformer	≤ 0.50% of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to "annually check and calibrate" does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to "annually check and calibrate" the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system

operator. Frequency inputs from other sources that are for reference only are excluded. The time error and frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

A. Introduction

1. **Title:** **Sabotage Reporting**

2. **Number:** CIP-001-2a

3. **Purpose:** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

   4.6. Transmission Owners (only in ERCOT Region).

   4.7. Generator Owners (only in ERCOT Region).

5. **Effective Date:** ERCOT Regional Variance will be effective the first day of the first calendar quarter after applicable regulatory approval.

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances. (Retired)

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4). (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance:

2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4. (Retired)

2.2. Level 2: Not applicable.

2.3. Level 3: Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. Level 4:.Not applicable.

E. ERCOT Interconnection-wide Regional Variance

Requirements

EA.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

EA.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

EA.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

EA.4. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall establish communications contacts with local Federal Bureau of Investigation (FBI) officials and develop reporting procedures as appropriate to their circumstances. (Retired)

Measures

M.A.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement EA1.

M.A.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements EA2 and EA3.

M.A.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to, procedures, policies, a letter of understanding, communication records,

or other equivalent evidence that will be used to confirm that it has established communications contacts with the local FBI officials to communicate sabotage events (Requirement EA4). (Retired)

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity shall be responsible for compliance monitoring.

1.2. Data Retention

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended
1	April 4, 2007	Regulatory Approval — Effective Date	New
1a	February 16, 2010	Added Appendix 1 — Interpretation of R2 approved by the NERC Board of Trustees	Addition
1a	February 2, 2011	Interpretation of R2 approved by FERC on February 2, 2011	Same addition
	June 10, 2010	TRE regional ballot approved variance	By Texas RE
	August 24, 2010	Regional Variance Approved by Texas RE Board of Directors	
2a	February 16, 2011	Approved by NERC Board of Trustees	

2a	August 2, 2011	FERC Order issued approving Texas RE Regional Variance	
2a	TBD	R4 and EA.4 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
CIP-001-1: **R2**. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.
Question
Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?
Response
The drafting team interprets the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. For example, reporting responsibilities result from NERC standards IRO-001 Reliability Coordination — Responsibilities and Authorities, COM-002-2 Communication and Coordination, and TOP-001 Reliability Responsibilities and Authorities, among others. Obligations to report could also result from agreements, processes, or procedures with other parties, such as may be found in operating agreements and interconnection agreements. The drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 Requirement R2. Regarding "who within the Interconnection hierarchy deems parties to be appropriate," the drafting team knows of no interconnection authority that has such a role.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-3

3. Purpose: Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-003-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-3 Requirement R2.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

	3	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within thirty calendar days of the effective date.	
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3. (Retired)	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1. (Retired)	LOWER	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
R3.2. (Retired)	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3. (Retired)	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	The Responsible Entity has established but not documented a change	The Responsible Entity has established but not documented both a change control process and configuration management	The Responsible Entity has not established and documented a change control process OR	The Responsible Entity has not established and documented a change control process AND

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		control process OR The Responsible Entity has established but not documented a configuration management process.	process.	The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a configuration management process.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-3a

3. Purpose: Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability

4.1. Within the text of Standard CIP-005-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-3, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-3 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity	

		shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation
3a	02/02/11	Approved by FERC	
3a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal

Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	and Standard CIP-009-4.	and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter.		
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6. (Retired)	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.			
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to designated response personnel.	Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	Revised.
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"
4a	4/19/12	FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3a, 4a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

3. Purpose: Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-007-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-3 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical)	

		Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
3	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, **but did not document** that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).

		testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).		
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.
R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program **but** did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.

R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.

R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
R5.1.1.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

			manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).		
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 **but** did not maintain records as specified in R7.3. (Retired)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A
R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3. (Retired)	LOWER	N/A	N/A	N/A	N/A

Formatted: Font color: Red

R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A
R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

E. **Regional Variances**

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Disturbance Reporting**

2. Number: EOP-004-1

3. Purpose: Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

4.6. Regional Reliability Organizations.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports. (Retired)

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1) (Retired)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1) (Retired)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1. (Retired)

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1	TBD	R1 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form EIA-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form EIA-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form EIA-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form EIA-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form EIA-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: ftp://ftp.eia.doe.gov/pub/electricity/eiafor417.doc.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
All DOE EIA-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE EIA-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				

All entities required to file a DOE EIA-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day
2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE EIA-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE EIA-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

A. Introduction

1. Title: **System Restoration from Blackstart Resources**

2. Number: EOP-005-2

3. Purpose: Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

4. Applicability:

4.1. Transmission Operators.

4.2. Generator Operators.

4.3. Transmission Owners identified in the Transmission Operators restoration plan.

4.4. Distribution Providers identified in the Transmission Operators restoration plan.

5. Proposed Effective Date: Twenty-four months after the first day of the first calendar quarter following applicable regulatory approval. In those jurisdictions where no regulatory approval is required, all requirements go into effect twenty-four months after Board of Trustees adoption.

B. Requirements

R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Time Horizon = Operations Planning]*

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

R1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

R1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.

R2. Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. *[Time Horizon = Operations Planning]*

R3. Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule. *[Time Horizon = Operations Planning]*

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary. (Retired)

R4. Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan. *[Time Horizon = Operations Planning]*

R4.1. Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.

R5. Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date. *[Time Horizon = Operations Planning]*

R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify: *[Time Horizon = Long-term Planning]*

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

R7. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each

affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration. *[Time Horizon = Real-time Operations]*

R8. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator. *[Time Horizon = Real-time Operations]*

R9. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Time Horizon = Operations Planning]*

R9.1. The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

R9.2. A list of required tests including:

R9.2.1. The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.

R9.2.2. The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

R9.3. The minimum duration of each of the required tests.

R10. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following: *[Time Horizon = Operations Planning]*

R10.1. System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.

R10.2. Restoration priorities.

R10.3. Building of cranking paths.

R10.4. Synchronizing (re-energized sections of the System).

R11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks. *[Time Horizon = Operations Planning]*

R12. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Time Horizon = Operations Planning]*

R13. Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. *[Time Horizon = Operations Planning]*

R14. Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. *[Time Horizon = Operations Planning]*

R15. Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator's restoration plan within 24 hours following such change. *[Time Horizon = Operations Planning]*

R16. Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. *[Time Horizon = Operations Planning]*

R16.1. Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R9.

R16.2. Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.

R17. Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: *[Time Horizon = Operations Planning]*

R17.1. System restoration plan including coordination with the Transmission Operator.

R17.2. The procedures documented in Requirement R14.

R18. Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator. *[Time Horizon = Operations Planning]*

C. Measures

M1. Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator.

M2. Each Transmission Operator shall have evidence such as e-mails with receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan in accordance with Requirement R2.

M3. Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, e-mails with receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.

M4. Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, e-mails with receipts, or registered mail receipts, that it has updated its restoration plan and submitted it to its Reliability Coordinator in accordance with Requirement R4.

M5. Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan available in its primary and backup control rooms and its System Operators prior to its implementation date in accordance with Requirement R5.

M6. Each Transmission Operator shall have documentation such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.

M7. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved shall have evidence such as voice recordings, e-mail, dated computer printouts, or operator logs, that it implemented its restoration plan or restoration plan strategies in accordance with Requirement R7.

M8. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved in such an event shall have evidence, such as voice recordings, e-mail, dated computer printouts, or operator logs, that it resynchronized shut down areas in accordance with Requirement R8.

M9. Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R9.

M10. Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R10.

M11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R11.

M12. Each Transmission Operator shall have evidence, such as training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R12.

M13. Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R13.

M14. Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R14.

M15. Each Generator Operator with a Blackstart Resource shall provide evidence, such as e-mails with receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within twenty-four hours of such changes in accordance with Requirement R15.

M16. Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R16.

M17. Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R17.

M18. Each Generator Operator shall have evidence, such as dated training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R18.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Approved restoration plan and any restoration plans in force since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of an updated restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three years for Requirement R4, Measure M4.
- The current, restoration plan approved by the Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- Implementation of its restoration plan or restoration plan strategies on any occasion for three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R7, Measure M7.
- Resynchronization of shut down areas on any occasion over three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R8, Measure M8.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R9, Measure M9.
- Actual training program materials or descriptions for three calendar years for Requirement R10, Measure M10.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit as well as one previous compliance audit period for Requirement R12, Measure M12.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator, applicable Transmission Owner, and applicable Distribution provider shall keep data or evidence to show compliance as identified

below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Actual training program materials or descriptions and actual training records for three calendar years for Requirement R11, Measure M11.

If a Transmission Operator, applicable Transmission owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in force since its last compliance audit for Requirement R13, Measure M13.

The Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current documentation and any documentation in force since its last compliance audit on procedures to start each Blackstart Resources and for energizing a bus for Requirement R14, Measure M14.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R15, Measure M15.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R16, Measure M16.
- Actual training program materials and actual training records for three calendar years for Requirement R17, Measure M17.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Generator Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R18, Measure M18.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	May 2, 2007	Approved by Board of Trustees	Revised
2	TBD	Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-005-2 (approval effective 5/23/11)	
2	TBD	R3.1 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Coordination of Plans For New Generation, Transmission, and End-User Facilities

2. Number: FAC-002-1

3. Purpose: To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.

4. Applicability:

4.1. Generator Owner

4.2. Transmission Owner

4.3. Distribution Provider

4.4. Load-Serving Entity

4.5. Transmission Planner

4.6. Planning Authority

5. (Proposed) Effective Date: The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:

1.1. Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.

1.2. Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.

1.3. Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.

1.4. Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.

1.5. Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected

transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days). (Retired)

C. Measures

M1. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider's documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.

M2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Timeframe

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting

Complaints

1.4. Data Retention

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

1.5. Additional Compliance Information

None

2. Violation Severity Levels (no changes)

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata
1	TBD	Modified to address Order No. 693 Directives contained in paragraph 693.	Revised.

1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Facility Ratings Methodology**

2. Number: FAC-008-1

3. Purpose: To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Transmission Owner

4.2. Generator Owner

5. Effective Date: August 7, 2006

B. Requirements

R1. The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:

R1.1. A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R1.2. The method by which the Rating (of major BES equipment that comprises a Facility) is determined.

R1.2.1. The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

R1.2.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R1.3. Consideration of the following:

R1.3.1. Ratings provided by equipment manufacturers.

R1.3.2. Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).

R1.3.3. Ambient conditions.

R1.3.4. Operating limitations.

R1.3.5. Other assumptions.

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request. (Retired)

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the

Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

C. Measures

M1. The Transmission Owner and Generator Owner shall each have a documented Facility Ratings Methodology that includes all of the items identified in FAC-008 Requirement 1.1 through FAC-008 Requirement 1.3.5.

M2. The Transmission Owner and Generator Owner shall each have evidence it made its Facility Ratings Methodology available for inspection within 15 business days of a request as follows: (Retired)

M2.1 The Reliability Coordinator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Reliability Coordinator Area. (Retired)

M2.2 The Transmission Operator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its portion of the Reliability Coordinator Area. (Retired)

M2.3 The Transmission Planner shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Transmission Planning Area. (Retired)

M2.4 The Planning Authority shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Planning Authority Area. (Retired)

M3. If the Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall have evidence that it provided a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Transmission Owner and Generator Owner shall self-certify its compliance to the Compliance Monitor at least once every three years. New Transmission Owners and Generator Owners shall each demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

The Transmission Owner and Generator Owner shall each keep all superseded portions of its Facility Ratings Methodology for 12 months beyond the date of the change in that methodology and shall keep all documented comments on the Facility Ratings Methodology and associated responses for three years. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant.

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Transmission Owner and Generator Owner shall each make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 Facility Ratings Methodology

1.4.2 Superseded portions of its Facility Ratings Methodology that had been replaced, changed or revised within the past 12 months

1.4.3 Documented comments provided by a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Authority on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology, and the associated responses

2. Levels of Non-Compliance

2.1. Level 1: There shall be a level one non-compliance if any of the following conditions exists:

2.1.1 The Facility Ratings Methodology does not contain a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.1.2 The Facility Ratings Methodology does not address one of the required equipment types identified in FAC-008 R1.2.1.

2.1.3 No evidence of responses to a Reliability Coordinator's, Transmission Operator, Transmission Planner, or Planning Authority's comments on the Facility Ratings Methodology. (Retired)

2.2. Level 2: The Facility Ratings Methodology is missing the assumptions used to determine Facility Ratings or does not address two of the required equipment types identified in FAC-008 R1.2.1.

2.3. Level 3: The Facility Ratings Methodology does not address three of the required equipment types identified in FAC-008-1 R1.2.1.

2.4. Level 4: The Facility Ratings Methodology does not address both Normal and Emergency Ratings ~~or the Facility Ratings Methodology was not made available for inspection within 15 business days of receipt of a request~~. (Deleted text retired)

Formatted: Strikethrough

E. **Regional Differences**

None Identified.

Version History

Version	Date	Action	Change Tracking
1	01/01/05	1. Lower cased the word "draft" and "drafting team" where appropriate. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Changed "Timeframe" to "Time	01/20/05

		Frame" and "twelve" to "12" in item D, 1.2.	
1	TBD	R2 and R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Facility Ratings**

2. **Number:** FAC-008-3

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.

4. **Applicability**

   4.1. Transmission Owner.

   4.2. Generator Owner.

5. **Effective Date:** The first day of the first calendar quarter that is twelve months beyond the date approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter twelve months following BOT adoption.

B. Requirements

R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:

- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
- Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:

2.2.1. Equipment Rating standard(s) used in development of this methodology.

2.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

2.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

2.2.4. Operating limitations.[1]

2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.4. The process by which the Rating of equipment that comprises a Facility is determined.

2.4.1. The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

2.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R3. Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

3.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:

3.2.1. Equipment Rating standard(s) used in development of this methodology.

[1] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

3.2.4. Operating limitations.[2]

3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

3.4. The process by which the Rating of equipment that comprises a Facility is determined.

3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R7. Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

[2] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

8.1. As scheduled by the requesting entities:

8.1.1. Facility Ratings

8.1.2. Identity of the most limiting equipment of the Facilities

8.2. Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1. Identity of the existing next most limiting equipment of the Facility

8.2.2. The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

C. Measures

M1. Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.

M2. Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.

M3. Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.

M4. Each Transmission Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement 4. The Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its documentation for determining its Facility Ratings or its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement R4. (Retired)

M5. If the Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology or a Generator Owner's documentation for determining its Facility Ratings, the Transmission Owner or Generator Owner shall have evidence, (such as a copy of a dated electronic or hard copy note, or other comparable evidence from the Transmission Owner or Generator Owner addressed to the commenter that includes the response to the comment,) that it provided a response to that commenting entity in accordance with Requirement R5. (Retired)

M6. Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).

M7. Each Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R7.

M8. Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability

Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority**

Regional Entity

1.2. **Compliance Monitoring and Enforcement Processes:**

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting
- Compliance Violation Investigations
- Complaints

1.3. **Data Retention**

The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.

The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.

The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.

The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.

The Generator Owner and Transmission Owner shall each keep evidence for Measure M4, and Measure M5, for three calendar years. (Retired)

The Generator Owner shall keep evidence for Measure M7 for three calendar years.

The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.

If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. **Additional Compliance Information**

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	• The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part 2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
R3	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	• 3.2.2 • 3.2.3 • 3.2.4	• 3.2.2 • 3.2.3 • 3.2.4	OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
R4 (Retired)	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.	The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.	The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)
R5 (Retired)	The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)	The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)	The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation. (R5)	The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
R7	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the requesting entities.
R8	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1)	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)	than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)

Formatted Table

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	
3	TBD	R4 and R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

A. Introduction

1. Title: **System Operating Limits Methodology for the Planning Horizon**

2. Number: FAC-010-2.1

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable planning of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Planning Authority

5. Effective Date: April 19, 2010

B. Requirements

R1. The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the planning horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R2.5. Starting with all Facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.6. In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:

R2.6.1. Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers.

R3. The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).

R3.2. Selection of applicable Contingencies.

R3.3. Level of detail of system models used to determine SOLs.

R3.4. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.5. Anticipated transmission system configuration, generation dispatch and Load level.

R3.6. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.

R4. The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:

R4.1. Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.

R4.2. Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.

R4.3. Each Transmission Planner that works in the Planning Authority's Planning Authority Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. Measures

M1. The Planning Authority's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Planning Authority shall have evidence it issued its SOL Methodology and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Planning Authority that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Planning Authority shall self-certify its compliance to the Compliance Monitor at least once every three years. New Planning Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Planning Authority shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

Formatted: Strikethrough

Formatted: Font color: Red

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Planning Authority shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology. (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R2.1 through R2.3 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.2	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
R2	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 –R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
R3	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
R4	One or both of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority failed to issue its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but

Requirement	Lower	Moderate	High	Severe
				four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
R5 (Retired)	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

E. **Regional Differences**

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-010.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
1	November 1, 2006	Fixed typo. Removed the word "each" from the 1st sentence of section D.1.3, Data Retention.	01/11/07
2	June 24, 2008	Adopted by Board of Trustees; FERC Order 705	Revised
2		Changed the effective date to July 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2.1	November 5, 2009	Adopted by the Board of Trustees — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	April 19, 2010	FERC Approved — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Operating Limits Methodology for the Operations Horizon**

2. Number: FAC-011-2

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: April 29, 2009

B. Requirements

R1. The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the operations horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. In determining the system's response to a single Contingency, the following shall be acceptable:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in FAC-011 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. Interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies

R2.3.3. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R3. The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)

R3.2. Selection of applicable Contingencies

R3.3. A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.

R3.3.1. This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies.

R3.4. Level of detail of system models used to determine SOLs.

R3.5. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.6. Anticipated transmission system configuration, generation dispatch and Load level

R3.7. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_V.

R4. The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:

R4.1. Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.

R4.2. Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.

R4.3. Each Transmission Operator that operates in the Reliability Coordinator Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. **Measures**

M1. The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Reliability Coordinator that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5 (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

Formatted: Strikethrough

Formatted: Font color: Red

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R3.1, R3.2, R3.4 through R3.7 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.1, R3.2, R3.4 through R3.7.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4.

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
R4	One or both of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to

Requirement	Lower	Moderate	High	Severe
				30 calendar days after the effectiveness of the change.
R5 (Retired)	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

2. Number: FAC-013-2

3. Purpose: To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.

4. Applicability:

4.1. Planning Coordinators

5. Effective Date:

In those jurisdictions where regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after applicable regulatory approval or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-2 are effective.

In those jurisdictions where no regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after Board of Trustees adoption or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1 and MOD-030-2 are effective.

B. Requirements

R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Criteria for the selection of the transfers to be assessed.

1.2. A statement that the assessment shall respect known System Operating Limits (SOLs).

1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's planning practices.

1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:

1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.

1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.

1.4.3. System demand.

1.4.4. Current approved and projected Transmission uses.

1.4.5. Parallel path (loop flow) adjustments.

1.4.6. Contingencies

1.4.7. Monitored Facilities.

1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.

R2. Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. Distribute to the following prior to the effectiveness of such revisions:

2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.

2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.

2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]* (Retired)

R4. During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

R5. Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

R6. If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

C. Measures

M1. Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.

M2. Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2

M3. Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. (Retired)

M4. Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.

M5. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5.

M6. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Data Retention

The Planning Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. (R3 retired)
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.

Formatted Table

Formatted Table

R2	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.
R3 **(Retired)**	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.

R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.

Formatted Table

R5	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.

Formatted Table

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	08/01/05	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Lower cased the word "draft" and "drafting team" where appropriate. 3. Changed Anticipated Action #5, page 1, from "30-day" to "Thirty-day." 4. Added or removed "periods."	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	5/17/12	FERC Order issued directing the VRF's for Requirements R1. and R4. be changed from "Lower" to "Medium." FERC Order issued correcting the High and Severe VSL language for R1.	
2	TBD	R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Interchange Confirmation**

2. Number: **INT-007-1**

3. Purpose: To ensure that each Arranged Interchange is checked for reliability before it is implemented.

4. Applicability

4.1. Interchange Authority.

5. Effective Date: January 1, 2007

B. Requirements

R1. The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:

R1.1. Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry. (Retired)

R1.3. The following are defined:

R1.3.1. Generation source and load sink.

R1.3.2. Megawatt profile.

R1.3.3. Ramp start and stop times.

R1.3.4. Interchange duration.

R1.4. Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.

C. Measures

M1. For each Arranged Interchange, the Interchange Authority shall show evidence that it has verified the Arranged Interchange information prior to the dissemination of the Confirmed Interchange.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Time Frame

The Performance-Reset Period shall be twelve months from the last noncompliance to Requirement 1.

1.3. Data Retention

The Interchange Authority shall keep 90 days of historical data. The Compliance Monitor shall keep audit records for a minimum of three calendar years.

1.4. Additional Compliance Information

Each Interchange Authority shall demonstrate compliance to the Compliance Monitor within the first year that this standard becomes effective or the first year the entity commences operation by self-certification to the Compliance Monitor.

Subsequent to the initial compliance review, compliance may be:

1.4.1 Verified by audit at least once every three years.

1.4.2 Verified by spot checks in years between audits.

1.4.3 Verified by annual audits of noncompliant Interchange Authorities, until compliance is demonstrated.

1.4.4 Verified at any time as the result of a complaint. Complaints must be lodged within 60 days of the incident. Complaints will be evaluated by the Compliance Monitor.

Each Interchange Authority shall make the following available for inspection by the Compliance Monitor upon request:

1.4.5 For compliance audits and spot checks, relevant data and system log records for the audit period which indicate an Interchange Authority's verification that all Arranged Interchange was balanced and valid as defined in R1. The Compliance Monitor may request up to a three-month period of historical data ending with the date the request is received by the Interchange Authority.

1.4.6 For specific complaints, only those data and system log records associated with the specific Interchange event contained in the complaint which indicate an Interchange Authority's verification that an Arranged Interchange was balanced and valid as defined in R1 for that specific Interchange

2. Levels of Non-Compliance

2.1. Level 1: One occurrence[1] where Interchange-related data was not verified as defined in R1.

2.2. Level 2: Two occurrences where Interchange-related data was not verified as defined in R1.

2.3. Level 3: Three occurrences where Interchange-related data was not verified as defined in R1.

2.4. Level 4: Four or more occurrences where Interchange-related data was not verified as defined in R1.

E. Regional Differences

None

[1] This does not include instances of not verifying due to extenuating circumstances approved by the Compliance Monitor.

Version History

Version	Date	Action	Change Tracking
1	TBD	R1.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Coordination of Real-time Activities Between Reliability Coordinators**

2. Number: **IRO-016-1**

3. Purpose: To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: November 1, 2006

B. Requirements

R1. The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.

R1.1. If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.

R1.2. If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).

R1.2.1. If time permits, this re-evaluation shall be done before taking corrective actions.

R1.2.2. If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

R1.3. If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both. (Retired)

C. Measures

M1. For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

The performance reset period shall be one calendar year.

1.3. Data Retention

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

1.4. Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction's discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

2. Levels of Non-Compliance

2.1. Level 1: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
Version 1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Hyphenated "30-day" and "Reliability Coordinator-to-Reliability Coordinator" when used as adjective.	01/20/06

		3. Changed standard header to be consistent with standard "Title." 4. Added "periods" to items where appropriate. 5. Initial capped heading "Definitions of Terms Used in Standard." 6. Changed "Timeframe" to "Time Frame" in item D, 1.2. 7. Lower cased all words that are not "defined" terms — drafting team, and self-certification. 8. Changed apostrophes to "smart" symbols. 9. Removed comma after word "condition" in item R.1.1. 10. Added comma after word "expected" in item 1.4, last sentence. 11. Removed extra spaces between words where appropriate.	
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Nuclear Plant Interface Coordination**

2. Number: NUC-001-2

3. Purpose: This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. Applicability:

4.1. Nuclear Plant Generator Operator.

4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

4.2.1 Transmission Operators.

4.2.2 Transmission Owners.

4.2.3 Transmission Planners.

4.2.4 Transmission Service Providers.

4.2.5 Balancing Authorities.

4.2.6 Reliability Coordinators.

4.2.7 Planning Coordinators.

4.2.8 Distribution Providers.

4.2.9 Load-serving Entities.

4.2.10 Generator Owners.

4.2.11 Generator Operators.

5. Effective Date: April 1, 2010

B. Requirements

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Medium*]

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

R4.1. Incorporate the NPIRs into their operating analyses of the electric system.

R4.2. Operate the electric system to meet the NPIRs.

R4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

R5. The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]

R9.1. Administrative elements: (Retired)

R9.1.1. Definitions of key terms used in the agreement. (Retired)

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. (Retired)

R9.1.3. A requirement to review the agreement(s) at least every three years. (Retired)

R9.1.4. A dispute resolution mechanism. (Retired)

R9.2. Technical requirements and analysis:

R9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

R9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

R9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

R9.3. Operations and maintenance coordination:

R9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

R9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

R9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

R9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

R9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. .

R9.3.6. Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

R9.3.7. Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

R9.4. Communications and training:

R9.4.1. Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

R9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

R9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

R9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

R9.4.5. Provisions for personnel training, as related to NPIRs.

C. Measures

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. (Requirement 2 and 9)

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:

M4.1 The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)

M4.2 The electric system was operated to meet the NPIRs. (Requirement 4.2)

M4.3 The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)

M8. The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

2.1. Lower: Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.

2.2. Moderate: Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.

2.3. High: One or more requirements of R3 through R8 were not met.

2.4. Severe: No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

E. Regional Differences

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs.
Therefore the definition of NPLR for Canadian CANDU units will be as follows:

Nuclear Plant Licensing Requirements (NPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	Revision
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update
2	TBD	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.**

2. Number: PRC-010-0

3. Purpose: Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.

4. Applicability:

4.1. Load-Serving Entity that operates a UVLS program

4.2. Transmission Owner that owns a UVLS program

4.3. Transmission Operator that operates a UVLS program

4.4. Distribution Provider that owns or operates a UVLS program

5. Effective Date: April 1, 2005

B. Requirements

R1. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).

R1.1. This assessment shall include, but is not limited to:

R1.1.1. Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.

R1.1.2. Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.

R1.1.3. A review of the voltage set points and timing.

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). (Retired)

C. Measures

M1. Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0_R1.

M2. Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

1.2. Compliance Monitoring Period and Reset Timeframe

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0_R1.1 or an assessment of the UVLS program was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

A. Introduction

1. **Title:** **Under-Voltage Load Shedding Program Performance**

2. **Number:** **PRC-022-1**

3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).

4. **Applicability**

   4.1. Transmission Operator that operates a UVLS program.

   4.2. Distribution Provider that operates a UVLS program.

   4.3. Load-Serving Entity that operates a UVLS program.

5. **Effective Date:** May 1, 2006

B. Requirements

R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UVLS set points and tripping times.

R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.

R1.4. A summary of the findings.

R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. (Retired)

C. Measures

M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.

M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization. (Retired)

D. Compliance

1. Compliance Monitoring Process

   1.1. Compliance Monitoring Responsibility

   Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

2.3. Level 3: Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

2.4. Level 4: Documentation of the analysis of UVLS performance was not provided.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	December 1, 2005	1. Removed comma after 2004 in "Development Steps Completed," #1. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Lower cased the word "region," "board," and "regional" throughout document where appropriate. 4. Added or removed "periods" where appropriate. 5. Changed "Timeframe" to "Time Frame" in item D, 1.2.	January 20, 2006
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Voltage and Reactive Control**

2. **Number:** VAR-001-2

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators.

   4.2. Purchasing-Selling Entities.

   4.3. Load Serving Entities.

5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.

R2. Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

R3. The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.

R3.1. Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.

R3.2. For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.

R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule [1] at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider. (Retired)

[1] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

R6. The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.

R6.1. When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.

R7. The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.

R8. Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.

R9. Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to support its voltage under first Contingency conditions.

R9.1. Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.

R10. Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.

R11. After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

R12. The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

C. Measures

M1. The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule as specified in Requirement 4 to each Generator Operator it requires to follow such a schedule.

M2. The Transmission Operator shall have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3.2.

M3. The Transmission Operator shall have evidence to show that it issued directives as specified in Requirement 6.1 when notified by a Generator Operator of the loss of an automatic voltage regulator control.

M4. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with Requirement 11.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months.

The Compliance Monitor shall retain any audit data for three years.

1.5. Additional Compliance Information

The Transmission Operator shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Violation Severity Levels (no changes)

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	TBD	Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised.
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan
Project 2013-02 – Paragraph 81

Requested Approvals

- None

Requested Retirements

- BAL-005-0.2b R2
- CIP-001-2a R4
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3
- CIP-003-3 R4.2
- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2
- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- EOP-004-1 R1
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-1 R2
- FAC-008-1 R3
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5
- FAC-011-2 R5
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5

Note that when these Requirements are retired, the version numbers of the standards will NOT be incremented, but the retired Requirements and associated elements will be clearly marked as retired. After evaluating the options and consulting with the Standards Committee and Standards Committee Process Subcommittee, the P81 drafting team determined that this was the most practical approach. Incrementing the version numbers of each standard is impractical because, in some cases, a subsequent version has already been developed. In addition, incrementing the version would require renumbering Requirements where a retired Requirement created a gap in numbering, and this creates an undesirable administrative burden for entities using certain systems to manage their compliance programs.

Prerequisite Approvals

- None

Revisions to Defined Terms in the NERC Glossary

- None

Background

On September 30, 2011, the North American Electric Reliability Corporation (NERC) filed a petition with the Federal Energy Regulatory Commission (FERC) requesting approval of its proposal to make informational filings in a "Find, Fix, Track and Report" (FFT) spreadsheet of lesser-risk, remediated possible violations of Reliability Standards. On March 15, 2012, the FERC issued an order conditionally accepting NERC's FFT proposal. In paragraph 81 (P81) of that order, the FERC stated:

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently. North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, a draft Standards Authorization Request (SAR) was drafted to set forth criteria and a process to identify Reliability Standard requirements that either: (a) provide little protection to the Bulk Electric System; (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file the identified Reliability Standard requirements with FERC to have them removed from the FERC-approved list of Reliability Standards.

Standards Process Input Group (SPIG)

In addition to addressing P81, the draft SAR was drafted consistent with what the SPIG developed as Recommendation No. 4, as set forth in NERC's Recommendations to Improve The Standards Development Process on page 12 (April 2012), which states:

> Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

Collaborative Process

The draft SAR and a suggested list of Reliability Standard requirements embedded in the SAR for consideration in the Initial Phase was the product of collaborative discussions among the following entities and their members: Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group. The draft SAR was posted for comment, which were due September 4, 2012. The P81 Standards Drafting Team reviewed the comments and finalized the SAR and the proposed list of Reliability Standard requirements for retirement.

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Authority
- Load Serving Entity
- NERC
- Planning Authority
- Planning Coordinator
- Purchasing-Selling Entity
- Regional Entity
- Regional Reliability Organization
- Reliability Coordinator
- Transmission Service Provider
- Transmission Operator
- Transmission Owner
- Transmission Planner

Effective Date of Retirements

All of the Requirements will be retired on the day of approval by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Note that no complete standard is being proposed for retirement and all of the other Requirements in each of the affected standards will remain in continuous effect until such time that the entire standard may be retired.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Retirement of Reliability Standard Requirements		
Date Submitted:	September 12, 2012		
SAR Requester Information			
Name:	Brian J. Murphy on behalf of the following:		
Organization:	P81 Interim Standards Drafting Team, as originally supported by Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group		
Telephone:	305-442-5132		
SAR Type (Check as many as applicable)			
☐ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated: "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser

SAR Information

risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, the problem this SAR is resolving is to identify Reliability Standards requirements that either: (a) provide little protection to the BPS;[1] (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file the identified Reliability Standard requirements with FERC to have them removed from the FERC-approved list of Reliability Standards.

In addition to addressing P81, this SAR is also consistent with Recommendation #4 set forth in *NERC's Recommendations to Improve The Standards Development Process* at page 12 (April 2012), which states:

> **Recommendation 4: Standards Product Issues** — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

[1] Given NERC's Reliability Standards are based on the definition of a Bulk Electric System (BES), the remainder of this SAR will use the term BES rather than Bulk Power System or BPS.

SAR Information
Purpose or Goal (How does this request propose to address the problem described above?):
The SAR addresses the problem identified above by: (1) Setting forth the initial phase-specific criteria (below) to evaluate whether a Reliability Standard requirement provides little protection to BES reliability or is unnecessary or redundant. (2) Establishing a multi-phased process for addressing these Reliability Standard requirements. During the initial phase, the standard drafting team will identify those Reliability Standard requirements that satisfy the criteria, set forth below, without the need for extensive technical justification or a modification to the requirement, and recommend the retirement of the requirement.[2] During subsequent phases, the standard drafting team may build upon the initial phase criteria, as applicable, to that phase that will identify the remaining appropriate Reliability Standard requirements that could not be included in the initial phase due to the need for additional analysis or a modification of language. This multi-phased approach is also proposed to address FERC's interest in increasing the efficiency of the ERO compliance program, so that the first set of identified Reliability Standard requirements may be filed with FERC on an expedited basis, and, therefore, start increasing ERO efficiencies as soon as practical. (3) At this time, the standard drafting team has identified a list of Reliability Standard requirements to be included in the initial phase that satisfy the criteria set forth below. (4) During each phase, as a list of Reliability Standard requirements is identified, the standard drafting team will also assist NERC staff to file these requirements with FERC so the requirements are removed from the FERC-approved list, including providing additional technical justification, as needed.

[2] The Standards Drafting Team will work with NERC staff to determine the manner to eliminate the identified Reliability Standard requirements.

SAR Information
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
The objectives of this SAR for all phases of this project are to retire or modify FERC-approved Reliability Standard requirements that provide little protection to the reliable operations of the BES, are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The scope of this SAR is all FERC-approved Reliability Standards.[3]
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The standard drafting team shall implement a phased process. The Initial Phase shall identify all FERC-approved Reliability Standard requirements that satisfy **both**: (i) Criteria A (the overarching criteria) and (ii) at least one of the Criteria B listed below (identifying criteria). In addition, for all phases, the standard drafting team shall also consider the data and reference points set forth below in Criterion C when deciding whether a Reliability Standard requirement should be retired or modified. **A. Overarching Criterion:** The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES. Section 215(a)(4) of the Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so

[3] The scope of this SAR with regard to those requirements that are proposed for retirement includes any currently pending versions of the listed Reliability Standards and any additional version of these Reliability Standards that may be submitted. In other words, the intent is to carry forward these retirements based on substance which is not dependent on the exact numbering or placement within a Reliability Standard.

SAR Information

that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

B. Identifying Criteria:

1. Administrative

The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

2. Data Collection/Data Retention

These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

3. Documentation

The Reliability Standard requirement requires responsible entities to develop a document (*e.g.,* plan, policy or procedure) which is not necessary to protect BES reliability.

4. Reporting

The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there would be little reliability impact.

5. Periodic Updates

The Reliability Standard requirement requires responsible entities to periodically update (*e.g.,* annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

6. Commercial or Business Practice

The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

SAR Information

7. Redundant

The Reliability Standard requirement is redundant with (i) another FERC-approved Reliability Standard requirement; (ii) the ERO compliance and monitoring program; or (iii) a governmental regulation (*e.g.,* Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

C. Additional data and reference points

In those instances where there is a need for additional information to assist in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B, the standard drafting team shall consider the following data and reference points to make a more informed decision:

1. Was the Reliability Standard requirement part of a Find, Fix and Track filing?

2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?

3. What is the Violation Risk Factor of the Reliability Standard requirement?

4. In which tier of the 2013 Actively Monitored List does the Reliability Standard requirement fall?

5. Is there a possible negative impact on NERC's published and posted reliability principles?

6. Is there any negative impact on the defense-in-depth protection of the BES?

7. Does the retirement promote results- or performance-based Reliability Standards?

To facilitate the standard drafting team's consideration of the above questions, NERC staff will provide the team with relevant known data and statistics.

SAR Information

List of Initial Phase Reliability Standard requirements that satisfy both Criteria A and B, with consideration of Criterion C

To be retired:[4]

BAL-005-0.2b R2

Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

Criterion B 7.

Statement:[5] BAL-005-0.2b is redundant with the Control Performance Standard defined in BAL-001-0.1a R1 and R2. This is also redundant in that it is measured by whether or not BAL-001-0.1a R1 and R2 are met.

Conclusion: This is redundant with the Control Performance Standard defined in BAL-001-0.1a R1 and R2. This is also redundant in that it is measured by whether or not BAL-001-0.1a R1 and R2 are met. This may be double jeopardy in that failure to achieve compliance with BAL-001-0.1a R1 and R2 could imply failure of this standard as well. This is misleading in requiring entities to maintain Regulating

[4] The following requirements that were originally presented in the draft SAR, and now in this final SAR are denoted with a "*" are so denoted because research shows that they are already scheduled to be retired via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the Board in November – *i.e.,* PRC-005-2), and, thus, are presented here for informational purposes only: COM-001-1.1 R6, EOP-009-0 R2; FAC-008-1 R1.3.5; PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; TOP-001-1a R3 and TOP-005-2a R1. These requirements are generally scheduled to be retired within the next year, and, therefore, to subject them to additional stakeholder vote, comment and Board of Trustees approval does not seem warranted or efficient. Consequently, these requirements will not be presented to stakeholders for comment and vote.

[5] The "Statement" and "Conclusion" sections are brief statements that provide context. The technical justification for each Reliability Standards requirement is contained in a separate Technical White Paper that will also be posted for comment.

SAR Information
Reserve, but providing no way to measurably comply, apart from achieving compliance with BAL-001-0.1a R1 and R2. **CIP-001-2a R4.** Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances. Criterion B 1, 2 and 3. **Statement:** CIP-001-2a is administrative, documentation and data collection in nature, because the establishment of communication contacts, in and of itself, with the FBI and RCMP has little or no impact on protection or the reliable operation of the BES. Instead, compliance with R1 through R3 of CIP-001-2a provides the actions that responsible entities take to protect the BES in the event of sabotage. Specifically, R1 through R3 require that the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity have procedures for the recognition of sabotage, reporting of sabotage and communication of sabotage events to appropriate parties in the Interconnection, which may include local law enforcement, the FBI, etc. Thus, CIP-001-2a R1 through R3 serve a reliability function, while R4 is a static, administrative requirement that has no clear results-based nexus to protecting the BES. **Conclusion**: Since this requirement provides little protection to the BES and is administrative in nature, Requirement 4 should be removed from Reliability Standard CIP-001-2a. **CIP-003-3, -4 R1.2** The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. Criterion B 1.

SAR Information

Statement: Whether there is a robust CIP compliance plan on which employees are trained may impact reliability, not whether the cyber security policy is readily available. Employees that are responsible for executing the cyber security policy are required to undergo a variety of training and follow multiple processes and procedures that are already required by the CIP requirements. Simply requiring that the policy be readily available is an administrative task that provides little, if any, benefit to reliability of the BES.

Conclusion: Since this requirement provides little protection to the BES and is purely administrative in nature, Requirement 1.2 should be removed from Reliability Standards CIP-003-3 and CIP-003-4.

CIP-003-3, -4 R3, R3.1, R3.2, R3.3

R3 Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1 Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2 Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3 Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Criterion B 1 and 3.

Statement: Over time, these exception requirements have proven to not be useful and have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements.

SAR Information

Conclusion: For regulatory efficiency, since these requirements provide little protection to the BES and are open to misinterpretation, in addition to being entirely documentation, Requirement 3 and its sub-requirements should be removed from Reliability Standards CIP-003-3 and CIP-003-4.

CIP-003-3, -4 R4.2.

The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Criterion B 1, 3 and 7.

Statement: CIP-003-3, -4 R4 already requires the classification of information associated with Critical Cyber Assets, which makes R4.2 redundant. The only difference in R4.2 is the term, "based on the sensitivity" has been added. The addition of this term can be viewed as overly managing the responsible entities' process of classification or simply not adding sufficient value to reliability to require a new requirement over and above R4.

Conclusion: Since this requirement is redundant and provides little protection to the BES, Requirement 4.2 should be removed from both Reliability Standards CIP-003-3 and CIP-003-4.

CIP-005-3a, -4a R2.6.

Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

Criterion B 1 and 3.

Statement: Over time, the banner requirement (or no trespass sign) has not been shown to be useful or consistent with a results-based approach to implementing a cyber security program. Additionally, it is administrative in nature.

SAR Information

Conclusion: Since this requirement provides little protection to the BES and is purely administrative in nature, Requirement R2 should be removed from Reliability Standards CIP-005-3a and CIP-005-4.

CIP-007-3, -4 R7.3

The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Criterion B 1 and 2.

Statement: CIP-007-3, -4 R7.3 is evidence collection and possible for inclusion in an RSAW.

Conclusion: Since this requirement provides little protection to the BES and is data collection in nature, it should be removed from CIP-007-3, -4.

***COM-001-1.1 R6.**

Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."

Criterion B 6 and 7.

Statement: This requirement has been approved by stakeholders for removal per Project 2006-06 (Reliability Coordination) and will be presented to the NERC Board of Trustees for approval in November. Thus, COM-001-1.1 R6 is presented here for informational purposes only.

EOP-004-1 R1.

Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

SAR Information
Criterion B 1 and 3. **Statement:** Whether or not there is a Regional Entity procedure to report disturbances has no impact on reliability. In other words, while a procedure for the collection of reports on disturbances may be useful information for purposes of Regional Entities to stay informed during events, is not an activity that protects the reliability of BES. The collection of such information should be established outside mandatory Reliability Standards. **Conclusion:** Since this requirement provides little protection to the BES and is purely documentation, Requirement 1 should be removed from Reliability Standard EOP-004-1. **EOP-005-2 R3.1**. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary. Criterion B 1, 5 and 7. **Statement:** EOP-005-2 R3 reads: "Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule." This requirement requires the Transmission Operator to submit its restoration plan to the Reliability Coordinator whether or not there have been changes. Therefore, R3.1 only adds a duplicative administrative burden for the entity to also confirm that there were no changes based upon another possible pre-determined schedule. Whether or not there was a change from year to year in the restoration plan will be documented in the revision history of the restoration plan, and thus the Reliability Coordinator will be able to ascertain whether or not there were changes based on R3. Thus, EOP-005-2 R3.1 provides little, if any, value to promoting the protection of the BES. **Conclusion:** For regulatory efficiency, and since this requirement appears redundant to R3, Requirement 3.1 should be removed from Reliability Standard EOP-005-2.

SAR Information

***EOP-009-0 R2.**

The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

Criterion B 4.

Statement: In Order No. 749, the Commission approved the retirement of EOP-009-0 R2 as of July 1, 2013, and, thus, it is presented here for informational purposes only.

FAC-002-1 R2.

The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

Criterion B 1 and 2.

Statement: Requiring the retention of studies for three years has no impact on protecting or the reliable operation of the BES, and is merely a data retention requirement that is better suited to be considered during an audit or in the context of compliance monitoring.

Conclusion: Since this requirement provides little protection to the BES and is purely data collection/retention, Requirement 2 should be removed from Reliability Standard FAC-002-1.

***FAC-008-1 R1.3.5.**

Other assumptions.

SAR Information

Criterion B 1.

Statement: The term “other assumptions" has already been removed via FAC-008-3, which will be effective on January 1, 2013, and, thus, it is presented here for informational purposes only.

FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5

FAC-008-1 R2 The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

FAC-008-1 R3 If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner’s or Generator Owner’s Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

FAC-008-3 R4 Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.

FAC-008-3 R5 If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner’s Facility Ratings methodology or Generator Owner’s documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.

SAR Information

Criterion B 1, 4 and 6.

Statement: For purposes of reliability, facility ratings are transmitted and used via the FAC (System Operating Limits), MOD and TPL Standards,[6] and posting the rating methodology for comment and responding to comments in and of itself has no reliability benefit. Furthermore, these requirements do not appear appropriate given the possible commercial or market related implications of sharing and debating with a competitor the facility ratings methodology of a facility.

Conclusion: For regulatory efficiency and possible commercial or market implications in sharing the facility ratings, and since these requirements are purely administrative in nature along with reporting activities, Requirements R2 and R3 of Reliability Standard FAC-008-1 and Requirements 4 and 5 of Reliability Standard FAC-008-3 should be removed from the Standards.

FAC-010-2.1 R5; FAC-011-2 R5

FAC-010-2.1 R5 If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

FAC-011-2 R5 If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

[6] MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-02 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element. Also, FAC-008-3 R7 and R8 require the transmission of facility ratings to reliability entities.

SAR Information
Criterion B 1, 4 and 6. **Statement:** A review of FAC-010-2.1 R5 and FAC-011-2 R5 indicate they are administrative requirements for the Planning Authority and Reliability Coordinator to respond to comments on its SOL methodology. Thus, similar to FAC-008-3 R4 and R5, there is no or little protection for BES reliability for a Planning Coordinator or Reliability Coordinator to enter into a give and take with the recipient on its SOL methodology. **Conclusion:** Since these requirements are purely administrative, FAC-010-2.1 R5 and FAC-011-2 R5 should be removed from the Standards. **FAC-013-2 R3** If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. Criterion B 1, 4 and 6. **Statement:** Similar to the concerns with FAC-008, the FAC-013-2 requirement to reply to comments on a transfer capability methodology has no reliability benefit, and, moreover, a back and forward on transfer capability could have commercial or market implications. **Conclusion:** For regulatory efficiency and possible commercial or market implications in sharing transfer capability methodology, and since these requirements are purely administrative in nature along with reporting activities, Requirement R3 of Reliability Standard FAC-013-2 should be removed from the Standards. **INT-007-1 R1.2**

SAR Information
All reliability entities involved in the Arranged Interchange are currently in the NERC registry. Criterion B 1. **Statement:** INT-007-1 R1.2 is administrative in nature, and adds little to reliability. **Conclusion:** Since INT-007-1 R1.2 provides little protection to the BES, it should be removed. **IRO-016-1 R2** The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both. Criterion B 1 and 2. **Statement:** IRO-016-1 R2 is an evidence requirement and is a candidate to go into an RSAW. **Conclusion:** Since IRO-016-1 R2 provides little protection to the BES and is data collection in nature, it should be removed. **NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4** R9.1 Administrative elements: R9.1.1 Definitions of key terms used in the agreement. R9.1.2 Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

SAR Information
R9.1.3 A requirement to review the agreement(s) at least every three years. R9.1.4 A dispute resolution mechanism. Criterion B 1. **Statement:** These requirements of NUC-001-2 do not address reliability, rather they address administrative and commercial terms of an agreement. Given there is no clear nexus between these requirements and reliability, they should be retired. **Conclusion:** Since these requirements are purely administrative in nature, provide for a periodic update and commercial terms of the agreement, they provide little protection to the BES. Requirement 9.1 and associated sub-requirements should be removed from Reliability Standard NUC-001-2. ***PRC-008-0 R1; *PRC-008-0 R2; *PRC-009-0 R1; *PRC-009-0 R1.1; *PRC-009-0 R1.2; *PRC-009-0 R1.3; *PRC-009-0 R1.4; *PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2.** PRC-008-0 R1 The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance. PRC-008-0 R2 The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days). PRC-009-0 R1 The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization)

SAR Information
shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to: PRC-009-0 R1.1 A description of the event including initiating conditions. PRC-009-0 R1.2 A review of the UFLS set points and tripping times. PRC-009-0 R1.3 A simulation of the event. PRC-009-0 R1.4 A summary of the findings. PRC-009-0 R2 The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event. PRC-010-0 R2 The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). PRC-022-1 R2 Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. Criterion B 1 and 2. **Statement:** Under Standards Development Project 2007-17 Protection System Maintenance, which recently passed on August 27, 2012, PRC-008-0 is scheduled to be retired and replaced with PRC-005-2.

SAR Information
PRC-005-2 will likely be presented to the NERC Board of Trustees in November for approval, and, thus, PRC-008-0 is only presented here for informational purposes. In Order No. 763 at Paragraph 103 the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Thus, PRC-009-0 is presented here for informational purposes only. Conversely, PRC-010-0 R2 and PRC-022-1 R2 are not scheduled to be retired and are purely administrative and data collection requirements that are better and more appropriately handled via spot checks/compliance audit request for evidence and the applicable RSAW. **Conclusion:** Since PRC-010-0 R2 and PRC-022-1 R2 provide little protection to the BES and better handled via the compliance and monitoring program. ***TOP-001-1a R3** Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions. Criterion B 7. **Statement:** Although there is redundancy between TOP-001-1a R3 and IRO-001-1a R8 related to Reliability Coordinators, this redundancy was addressed in Standards Development Project 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces TOP-001-1a R3 and reads: Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued and identified as such by its

SAR Information

Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.

TOP-001-2 has been approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-001-1a R3 is presented for informational purposes only.

***TOP-005-2a R1**

As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."

Criterion B 3.

Statement:

TOP-005-2a R1 is better suited for ROP than reliability requirement. A review of Standards Development Project 2007-03 Real-time Transmission Operations indicates it proposes R1 of TOP-005-1 to be retired. As stated above in the context of TOP-001, this project was approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-005-2a R1 is presented for informational purposes only.

Conclusion: Since TOP-005-2a R1 provides little protection to the BES and is purely documentation in nature, it should be removed.

VAR-001-2 R5

Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

Criterion B 7.

SAR Information
Statement: VAR-001-2 R5 is redundant with FERC's pro forma open access transmission tariff (OATT) Specifically, the requirement provides for the PSE and LSE to arrange for reactive resources to satisfy the reactive requirements of the Transmission Service Provider, which is already required under Schedule No. 2 of the OATT. **Conclusion**: Since VAR-001-2 R5 is redundant with requirements already under FERC's OATT, and, thus, it should be removed.

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☒	Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of responsible entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☒	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☒	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☒	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk

Reliability Functions		
		Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☒	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.

Reliability and Market Interface Principles	
☒	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation

Related SARs	
SAR ID	Explanation

Related SARs	

Regional Variances	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Retirement of Reliability Standard Requirements		
Date Submitted:	September 12~~June 29~~, 2012		
SAR Requester Information			
Name:	Brian J. Murphy on behalf of the following:		
Organization:	P81 Interim Standards Drafting Team, as originally supported by Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group		
Telephone:	305-442-5132		
SAR Type (Check as many as applicable)			
☐ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated: "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser

SAR Information

risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, the problem this SAR is resolving is to identify Reliability Standards requirements that either: (a) provide little protection to the BPS;[1] (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file the identified Reliability Standard requirements with FERC to have them removed from the FERC-approved list of Reliability Standards.

In addition to addressing P81, this SAR is also consistent with Recommendation #4 set forth in *NERC's Recommendations to Improve The Standards Development Process* at page 12 (April 2012), which states:

> **Recommendation 4: Standards Product Issues** — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

[1] Given NERC's Reliability Standards are based on the definition of a Bulk Electric System (BES), the remainder of this SAR will use the term BES rather than Bulk Power System or BPS.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
Purpose or Goal (How does this request propose to address the problem described above?):
The SAR addresses the problem identified above by: (1) Setting forth the initial phase-specific criteria (below) to evaluate whether a Reliability Standard requirement provides little protection to BES reliability or is unnecessary or redundant. (2) Establishing a multi-phased process for addressing these Reliability Standard requirements. During the initial phase~~Initial Phase~~, the standard drafting team~~Standards Drafting Team~~ will identify those Reliability Standard requirements that ~~easily~~ satisfy the criteria, set forth below, without the need for extensive technical justification or a modification to the requirement, and ~~either~~ recommend~~: (a)~~ the retirement of the requirement.[2] During subsequent[3] ~~or (b) a modification to the requirement,~~[4] ~~while future~~ phases, the standard drafting team may build upon the initial phase criteria, as applicable, to that phase that will identify the remaining appropriate Reliability Standard requirements that ~~satisfy the criteria, but~~ could not be included in the initial phase~~Initial Phase~~ due to the need for additional analysis or a modification of language. This multi-phased approach is also proposed to address FERC's interest in increasing the efficiency of the ERO compliance program, so that the first set of identified Reliability Standard requirements may be filed with FERC on an expedited basis, and, therefore, start increasing ERO efficiencies as soon as practical. (3) At this time,~~To facilitate~~ the standard drafting team has identified~~Initial Phase of the Standard Drafting Team's process,~~ a list of Reliability Standard requirements to be included in the initial phase that ~~appear to easily~~ satisfy the criteria ~~are~~ set forth below.

[2] The Standards Drafting Team will work with NERC staff to determine the manner to eliminate the identified Reliability Standard requirements.

[3] ~~The Standards Drafting Team will work with NERC staff to determine the manner to eliminate the identified Reliability Standards requirements.~~

[4] ~~Given the expedited nature of the Initial Phase, it is unlikely there will be a large number of modifications considered, and the Standards Drafting Team may decide to defer all requested modifications to subsequent phases.~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
(4) During each phase, as a list of Reliability Standard requirements is identified, the standard drafting team ~~and passes through the Standards Development Process, the Standards Drafting Team~~[5] will also assist NERC staff to file these requirements with FERC so the requirements are removed from the FERC-approved list, including providing additional technical justification, as needed.
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
The objectives of this SAR for all phases of this project are to retire or modify FERC-approved Reliability Standard requirements that provide little protection to the reliable operations of the BES, are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The scope of this SAR is all FERC-approved Reliability Standards.[6]
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The standard drafting team~~Standard Drafting Team~~ shall implement a phased process. The Initial Phase shall identify all FERC- approved Reliability Standard requirements that ~~easily satisfy the criteria set forth below, while future phases shall identify FERC-approved Reliability Standard requirements that satisfy the criteria set forth below, but could not be included in the Initial Phase due to the need for additional analysis or an editing of language. During each phase the Standards Drafting Team shall~~

~~[5] While this SAR applies to all phases of the P81 project, it is understood that the composition of the Standard Drafting Team may need to change or be supplemented in subsequent phases depending on the technical expertise required.~~

[6] The scope of this SAR with regard to those requirements that are proposed for retirement includes any currently pending versions of the listed Reliability Standards and any additional version of these Reliability Standards that may be submitted. In other words, the intent is to carry forward these retirements based on substance which is not dependent on the exact numbering or placement within a Reliability Standard.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

~~identify Reliability Standard requirements that~~ satisfy **both**: (i) Criteria A ~~(~~) ~~the~~ overarching criteria) and (ii~~B~~) at least one of the Criteria B listed below (identifying~~technical~~ criteria). ~~.~~ In addition, for all phases, the standard drafting team~~Standards Drafting Team~~ shall also consider the data and reference points set forth below in Criterion C when deciding whether a Reliability Standard requirement should be retired or modified.

A. Overarching Criterion:

The~~In the event no responsible entity performed the FERC-approved~~ Reliability Standard requirement requires responsible entities to conduct an activity or task that does~~, there would be~~ little, if anything, ~~or no impact~~ to benefit~~the protection~~ or protect the reliable operation of the BES.

Formatted: Right: 0.5"

Section 215(a)(4) of the Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

B. Identifying~~Technical~~ Criteria:

1. Administrative

The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

2. Data Collection/Data Retention

~~The Reliability Standard requirement requires responsible entities to collect or retain data and does not contribute to: (a) the reliable operation of the BES or (b) an effective compliance enforcement processes.~~ These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes ~~or addressed in the data retention sections of Reliability Standards~~.

3. ~~Purely~~ Documentation

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
The Reliability Standard requirement requires responsible entities to develop a document (*e.g.,* plan, policy or procedure) which is not necessary to protect BES reliability.
4. ~~Purely~~ Reporting The Reliability Standard requirement obligates responsible entities to report ~~out~~ to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible ~~discernable~~ impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there ~~it~~ would be ~~have~~ little reliability impact ~~on the reliable operation of the BES~~.
5. Periodic Updates The Reliability Standard requirement requires responsible entities to periodically update (*e.g.,* annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.
6. Commercial or Business Practice The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues. ~~*e.g.,* better served as a NAESB standard or as part of NAESB Electric Industry Registry (EIR).~~
7. Redundant The Reliability Standard requirement is redundant with (i) ~~either~~ another FERC-approved Reliability Standard requirement; (ii) the ERO compliance and monitoring program; or (iii) a ~~or~~ governmental regulation (*e.g.,* Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), ~~,~~ etc.).
~~**8. Hinders the protection or reliable operation of the BES**~~ ~~The Reliability Standard requirement requires responsible entities to conduct an activity or task that hinders, distracts or is counterproductive to the protection or reliable operation of the BES.~~
~~**9. Little, if any, value as a reliability requirement**~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

~~The tasks or activities in the Reliability Standard requirement do little, if anything, to promote the protection the BES.~~

C. Additional data and reference points

In those instances where~~when~~ there is a~~the~~ need for additional information to assist in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B, the standard drafting team~~Standards Drafting Team~~ shall consider the following data and reference points to make a more informed decision:

1. Was the Reliability Standard requirement part of a Find, Fix and Track filing?

2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?

3. What is the Violation Risk Factor of the Reliability Standard requirement?

4. In which tier of the 2013 Actively Monitored List~~Standards~~ does the Reliability Standard requirement fall?

5. Is there a possible~~Any~~ negative impact on NERC's published and posted reliability principles?

6. Is there any~~Any~~ negative impact on the defense-in-depth protection of the BES?

7. Does the retirement ~~or modification~~ promote results- or performance-based Reliability Standards?

To facilitate the standard drafting team's~~Standard Drafting Team's~~ consideration of the above questions, NERC staff will provide the team with relevant known data and statistics.

Formatted: Font: Bold

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

List of Initial Phase~~To facilitate the Standard Drafting Team's Initial Phase, below is a list of Reliability Standard requirements that appear to satisfy both Criteria A and B, with consideration of Criterion C. To assist the Team's review of these requirements, Criterion B coding is provided, along with a brief statement explaining why the requirement provides little protection to the BES, is unnecessary or is redundant.~~

~~List of Phase One~~ Reliability Standard requirements that satisfy both Criteria A and B, with consideration of Criterion C

To be retired:[7]

BAL-005-0.2b~~1b~~ R2

Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

Criterion B 7.

Statement:[8] BAL-005-0.2b~~1b~~ is redundant with the Control Performance Standard defined in BAL-001-0.1a R1 and R2. This is also redundant in that it is measured by whether or not BAL-001-0.1a R1 and R2

[7] The following requirements that were originally presented in the draft SAR, and now in this final SAR are denoted with a "*" are so denoted because research shows that they are already scheduled to be retired via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the Board in November – *i.e.*, PRC-005-2), and, thus, are presented here for informational purposes only: COM-001-1.1 R6, EOP-009-0 R2; FAC-008-1 R1.3.5; PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; TOP-001-1a R3 and TOP-005-2a R1. These requirements are generally scheduled to be retired within the next year, and, therefore, to subject them to additional stakeholder vote, comment and Board of Trustees approval does not seem warranted or efficient. Consequently, these requirements will not be presented to stakeholders for comment and vote.

Formatted: Font: Not Bold

Formatted: Left

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

are met.

Conclusion: This is redundant with the Control Performance Standard defined in BAL-001-0.1a R1 and R2. This is also redundant in that it is measured by whether or not BAL-001-0.1a R1 and R2 are met. This may be double jeopardy in that failure to achieve compliance with BAL-001-0.1a R1 and R2 could imply failure of this standard as well. This is misleading in requiring entities to maintain Regulating Reserve, but providing no way to measurably comply, apart from achieving compliance with BAL-001-0.1a R1 and R2.

CIP-001-2a -R4.

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

Criterion B 1, 2~~, 3, 8~~ and 3~~9~~.

Statement: CIP-001-2a is administrative, documentation and data collection in nature, because the establishment of communication contacts, in and of itself, with the FBI and RCMP has little or no impact on protection or the reliable operation of the BES. Instead, compliance with R1 through -R3 of CIP-001-2a provides the actions that responsible entities take to protect the BES in the event of sabotage. Specifically, R1 through R3 require that the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity ~~to~~ have procedures for the recognition of sabotage, reporting of sabotage and communication of sabotage events to appropriate parties in the Interconnection, which may include local law enforcement, the FBI, etc. Thus, ~~in~~ CIP-001-2a~~,~~ R1 through R3 serve a reliability function, while R4 is a static, administrative requirement that has no clear results-based nexus to protecting the BES.~~Bulk Electric System (BES).~~

[8] The "Statement" and "Conclusion" sections are brief statements that provide context. The technical justification for each Reliability Standards requirement is contained in a separate Technical White Paper that will also be posted for comment.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
Conclusion: Since this requirement provides little protection to the BES and is administrative in nature, Requirement 4 should be removed from Reliability Standard CIP-001-2a. **CIP-003-3, -4 R1.2** The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. Criterion B 1. **Statement:** Whether there is a robust CIP compliance plan on which employees are trained -may impact reliability, not whether the cyber security policy is readily available. Employees that are responsible for executing the cyber security policy are required to undergo a variety of training and, follow multiple processes and procedures that are already required by the CIP requirements. Simply requiring that the policy be readily available is an administrative task that provides little, if any, benefit to reliability of the BES. **Conclusion:** Since this requirement provides little protection to the BES and is purely administrative in nature, Requirement 1.2 should be removed from Reliability Standards CIP-003-3 and CIP-003-4. **CIP-003-3, -4 R3, R3.1, R3.2, R3.3** R3 Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). R3.1 Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). R3.2 Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. R3.3 Authorized exceptions to the cyber security policy must be reviewed and approved

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. Criterion B 1~~, 3~~ and 3~~8~~. **Statement:** Over time, these exception requirements have proven to not be useful and have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements. **Conclusion:** For regulatory efficiency, since these requirements provide little protection to the BES and are open to misinterpretation, in addition to being entirely documentation, Requirement 3 and its sub-requirements~~subrequirements~~ should be removed from Reliability Standards~~Standard~~ CIP-003-3 and CIP-003-4. **CIP-003-3, -4 R4.2.** The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. Criterion B 1, 3 and 7. **Statement:** CIP-003-3, -4 R4 already requires the classification of information associated with Critical Cyber Assets, which makes R4.2 redundant. The only difference in R4.2 is the term, "based on the sensitivity" has been added. The addition of this term can be viewed as overly managing the responsible entities' process of classification or simply not adding sufficient value to reliability to require a new requirement over and above R4. **Conclusion:** Since this requirement is~~these requirements are~~ redundant and provides~~provide~~ little protection to the BES, Requirement 4.2 should be removed from both Reliability Standards CIP-003-3 and CIP-003-4.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
CIP-005-3a, -4a R2.6. Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. ~~devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.~~ Criterion B 1~~, 3, 8~~ and 3~~9~~. **Statement:** Over time, the banner requirement (or no trespass sign) has not been shown to be useful or consistent with a results-based approach to implementing a cyber security program. Additionally, it is administrative in nature. **Conclusion:** Since this requirement provides little protection to the BES and is purely administrative in nature, Requirement R2 should be removed from Reliability Standards CIP-005-3a and CIP-005-4. **CIP-007-3, -4 R7.3** The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. Criterion B 1 and 2. **Statement:** CIP-007-3, -4 R7.3 is evidence collection and possible for inclusion in an RSAW. **Conclusion:** Since this requirement provides little protection to the BES and is data collection in nature, it should be removed from CIP-007-3, -4. ***COM-001-1.1 R6.**

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy." Criterion B 6 and 7. **Statement:** ~~Whether the entity has a robust up-to-date CIP compliance plan may impact reliability, but not whether it employs a specific business practice such as the NERCNet. NOTE:~~ This requirement has been approved by stakeholders~~is proposed~~ for removal per Project 2006-06 (Reliability Coordination) and will ~~with the rationale: "The RC SDT is recommending that R6~~ be presented to the NERC Board of Trustees for approval~~retired. This is an ERO procedural issue and should not be~~ in November. Thus,~~a reliability standard. It should be included in the ERO Rules of Procedure."~~ ~~**Conclusion:** Since this requirement provides little protection to the BES and is more appropriate as a Commercial and Business Practice, Requirement 6 should be removed from Reliability Standard~~ COM-001-1.1 R6 is presented here for informational purposes only. **EOP-004-1 R1.** Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports. Criterion B 1~~, 3~~ and 3~~4~~. **Statement:** Whether or not there is a Regional Entity procedure to report disturbances has no impact on reliability. In other words, while a procedure for the collection of reports on disturbances may be useful information for purposes of Regional Entities to stay informed during events, is not an activity that protects the reliability of BES. The collection of such information should be established outside mandatory Reliability Standards. **Conclusion:** Since this requirement provides little protection to the BES and is purely documentation, Requirement 1 should be removed from Reliability Standard EOP-004-1.

Formatted: Highlight

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

EOP-005-2 R3.1.

If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

Criterion B 1, 5~~, 7~~ and 79.

Statement: EOP-005-2 R3 reads: "Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule." This requirement requires the Transmission Operator to submit its restoration plan to the Reliability Coordinator whether or not there have been changes. Therefore, R3.1 only adds a duplicative administrative burden for the entity to also confirm that there were no changes based upon another possible pre-determined schedule. Whether or not there was a change from year to year in the restoration plan will be documented in the revision history of the restoration plan, and thus the Reliability Coordinator will be able to ascertain whether or not there were changes based on R3. Thus, EOP-005-2 R3.1 provides little, if any, value to promoting the protection of the BES.

Conclusion: For regulatory efficiency, and since this requirement appears redundant to R3, Requirement 3.1 should be removed from Reliability Standard EOP-005-2.

***EOP-009-0 R2.**

The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

Criterion B 4.

Statement: In Order No. 749, the Commission approved the retirement of EOP-009-0 R2 as of July 1, 2013, and, thus, it is presented here for informational purposes only.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

~~**Statement:** The requirement to report blackstart test results to the Regional Entity and NERC has no impact on reliability. If the Regional Entity desires to review or track this information, a better vehicle to obtain it is via a Compliance Audit or Spot-Check, or some other compliance monitoring procedure.~~

~~**Conclusion:** For regulatory efficiency and since this requirement is purely a reporting activity, Requirement 2 should be removed from Reliability Standard EOP-009-0.~~

FAC-002-1 R2.

The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

Criterion B 1~~2, 3~~ and 2~~4~~.

Statement: Requiring the retention of studies for three years has no impact on protecting or the reliable operation of the BES, and is merely a data retention requirement that is better suited to be considered during an audit or in the context of compliance monitoring.

Conclusion: Since this requirement provides little protection to the BES and is purely data collection/retention, Requirement 2 should be removed from Reliability Standard FAC-002-1.

***FAC-008-1 R1.3.5.**

Other assumptions.

Criterion B 1~~8~~.

Statement: The term “other assumptions" has already been removed via FAC-008-3, which will be

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

effective on January 1, 2013, and, thus, it is presented here for informational purposes only~~in the context of facility ratings is very close to meaningless from a technical standpoint, generic and, therefore, yields no protection of the BES~~.

~~**Conclusion:** Since this requirement provides little or no protection to the BES and is unnecessary, Requirement 1.3.5 should be removed from Reliability Standard FAC-008-1.~~

FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5

FAC-008-1 R2 The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

FAC-008-1 R3 If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

FAC-008-3 R4 Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.

FAC-008-3 R5 If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. Criterion B 1, ~~2,~~ 4 and 6. **Statement:** For purposes of reliability, facility ratings are transmitted and used via the FAC (System Operating Limits), MOD and TPL Standards,[9] and posting the rating methodology for comment and responding to comments in and of itself has no reliability benefit. Furthermore, these requirements do not appear appropriate given the possible commercial or market related implications of sharing and debating with a competitor the facility ratings methodology of a facility. **Conclusion:** For regulatory efficiency and possible commercial or market implications in sharing the facility ratings, and since these requirements are purely administrative in nature along with reporting activities, Requirements R2 and R3 of Reliability Standard FAC-008-1 and Requirements 4 and 5 of Reliability Standard FAC-008-3 should be removed from the Standards. **FAC-010-2.1 R5; FAC-011-2 R5** FAC-010-2.1 R5 If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. FAC-011-2 R5 If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason

Formatted: Tab stops: 0.5", Left

[9] MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-02 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element. Also, FAC-008-3 R7 and R8 require the transmission of facility ratings to reliability entities.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

why.

Criterion B 1, 4 and 6.

Statement: A review of FAC-010-2.1 R5 and FAC-011-2 R5 indicate they are administrative requirements for the Planning Authority and Reliability Coordinator to respond to comments on its SOL methodology. Thus, similar to FAC-008-3 R4 and R5, there is no or little protection for BES reliability for a Planning Coordinator or Reliability Coordinator to enter into a give and take with the recipient on its SOL methodology.

Conclusion: Since these requirements are purely administrative, FAC-010-2.1 R5 and FAC-011-2 R5 should be removed from the Standards.

FAC-013-2 R3

If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.

Criterion B 1, ~~2,~~ 4 and 6.

Statement: Similar to the concerns with FAC-008, the FAC-013-2 requirement to reply to comments on a transfer capability methodology has no reliability benefit, and, moreover, a back and forward on transfer capability could have commercial or market implications.

Conclusion: For regulatory efficiency and possible commercial or market implications in sharing transfer capability methodology, and since these requirements are purely administrative in nature along with reporting activities, Requirement R3 of Reliability Standard FAC-013-2 should be removed from the Standards.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

INT-007-1 R1.2

All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

Criterion B 1.

Statement: INT-007-1~~,~~ R1.2 is administrative in nature, and adds little to reliability.

Conclusion: Since INT-007-1 R1.2 provides little protection to the BES, it should be removed.

IRO-016-1 R2

The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

Criterion B 1 and 2.

Statement:

IRO-016-1 R2 is an evidence requirement and is a candidate~~. Candidate~~ to go into an RSAW.

Conclusion: Since IRO-016-1 R2 provides little protection to the BES and is data collection in nature, it should be removed.

~~MOD-004-1 R1; MOD-004-1 R1.1; MOD-004-1 R1.2; MOD-004-1 R1.3; MOD-004-1 R2; MOD-004-1 R3; MOD-004-1 R3.1; MOD-004-1 R3.2; MOD-004-1 R4; MOD-004-1 R4.1; MOD-004-1 R4.2; MOD-004-1 R5; MOD-004-1 R5.1; MOD-004-1 R5.2; MOD-004-1 R6; MOD-004-1 R6.1; MOD-004-1 R6.2; MOD-004-1 R7; MOD-004-1 R8; MOD-004-1 R9; MOD-004-1 R9.1; MOD-004-1 R9.2; MOD-004-1 R10; MOD-004-1 R11; MOD-004-1 R12; MOD-004-1 R12.1; MOD-004-1 R12.2; MOD-004-1 R12.3.~~

~~R1 The Transmission Service Provider that maintains CBM shall prepare and keep current a "Capacity~~

Formatted: Tab stops: Not at 1.5"

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
~~Benefit Margin Implementation Document" (CBMID) that includes, at a minimum, the following information: [Time Horizon: Operations Planning, Long-term Planning]~~ ~~R1.1. The process through which a Load-Serving Entity within a Balancing Authority Area associated with the Transmission Service Provider, or the Resource Planner associated with that Balancing Authority Area, may ensure that its need for Transmission capacity to be set aside as CBM will be reviewed and accommodated by the Transmission Service Provider to the extent Transmission capacity is available.~~ ~~R1.2. The procedure and assumptions for establishing CBM for each Available Transfer Capability (ATC) Path or Flowgate.~~ ~~R1.3. The procedure for a Load-Serving Entity or Balancing Authority to use Transmission capacity set aside as CBM, including the manner in which the Transmission Service Provider will manage situations where the requested use of CBM exceeds the amount of CBM available.~~ ~~R2. The Transmission Service Provider that maintains CBM shall make available its current CBMID to the Transmission Operators, Transmission Service Providers, Reliability Coordinators, Transmission Planners, Resource Planners, and Planning Coordinators that are within or adjacent to the Transmission Service Provider's area, and to the Load Serving Entities and Balancing Authorities within the Transmission Service Provider's area, and notify those entities of any changes to the CBMID prior to the effective date of the change. [Time Horizon: Operations Planning]~~ ~~R3. Each Load-Serving Entity determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by: [Time Horizon: Operations Planning]~~ ~~R3.1. Using one or more of the following to determine the GCIR:~~ ~~Loss of Load Expectation (LOLE) studies~~ ~~Loss of Load Probability (LOLP) studies~~ ~~Deterministic risk-analysis studies~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
~~Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities~~ ~~R3.2. Identifying expected import path(s) or source region(s).~~ ~~R4. Each Resource Planner determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by: [Time Horizon: Operations Planning]~~ ~~R4.1. Using one or more of the following to determine the GCIR:~~ ~~Loss of Load Expectation (LOLE) studies~~ ~~Loss of Load Probability (LOLP) studies~~ ~~Deterministic risk-analysis studies~~ ~~Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities~~ ~~R4.2. Identifying expected import path(s) or source region(s).~~ ~~R5. At least every 13 months, the Transmission Service Provider that maintains CBM shall establish a CBM value for each ATC Path or Flowgate to be used for ATC or Available Flowgate Capability (AFC) calculations during the 13 full calendar months (months 2-14) following the current month (the month in which the Transmission Service Provider is establishing the CBM values). This value shall: [Time Horizon: Operations Planning]~~ ~~R5.1. Reflect consideration of each of the following if available:~~ ~~Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Service Provider's area~~ ~~Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
~~Service Provider's area~~ ~~Any reserve margin or resource adequacy requirements for loads within the Transmission Service Provider's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities~~ ~~R5.2 Be allocated as follows:~~ ~~For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners~~ ~~For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Service Provider~~ ~~R6 At least every 13 months, the Transmission Planner shall establish a CBM value for each ATC Path or Flowgate to be used in planning during each of the full calendar years two through ten following the current year (the year in which the Transmission Planner is establishing the CBM values). This value shall: [Time Horizon: Long-term Planning]~~ ~~R6.1 Reflect consideration of each of the following if available:~~ ~~Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Planner's area~~ ~~Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Planner's area~~ ~~Any reserve margin or resource adequacy requirements for loads within the Transmission Planner's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities~~ ~~R6.2 Be allocated as follows:~~ ~~For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

~~For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Planner.~~

~~R7. Less than 31 calendar days after the establishment of CBM, the Transmission Service Provider that maintains CBM shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the Transmission Service Provider's system of the amount of CBM set aside. [Time Horizon: Operations Planning]~~

~~R8. Less than 31 calendar days after the establishment of CBM, the Transmission Planner shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the system being planned by the Transmission Planner of the amount of CBM set aside. [Time Horizon: Operations Planning]~~

~~R9. The Transmission Service Provider that maintains CBM and the Transmission Planner shall each provide (subject to confidentiality and security requirements) copies of the applicable supporting data, including any models, used for determining CBM or allocating CBM over each ATC Path or Flowgate to the following: [Time Horizon: Operations Planning, Long-term Planning]~~

~~R9.1. Each of its associated Transmission Operators within 30 calendar days of their making a request for the data.~~

~~R9.2. To any Transmission Service Provider, Reliability Coordinator, Transmission Planner, Resource Planner, or Planning Coordinator within 30 calendar days of their making a request for the data.~~

~~R10. The Load-Serving Entity or Balancing Authority shall request to import energy over firm Transfer Capability set aside as CBM only when experiencing a declared NERC Energy Emergency Alert (EEA) 2 or higher. [Time Horizon: Same-day Operations]~~

~~R11. When reviewing an Arranged Interchange using CBM, all Balancing Authorities and Transmission Service Providers shall waive, within the bounds of reliable operation, any Real-time timing and ramping~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

~~requirements. [Time Horizon: Same-day Operations]~~

~~R12. The Transmission Service Provider that maintains CBM shall approve, within the bounds of reliable operation, any Arranged Interchange using CBM that is submitted by an "energy deficient entity" under an EEA 2 if: [Time Horizon: Same-day Operations]~~

~~R12.1. The CBM is available~~

~~R12.2. The EEA 2 is declared within the Balancing Authority Area of the "energy deficient entity," and~~

~~R12.3. The Load of the "energy deficient entity" is located within the Transmission Service Provider's area.~~

~~Criterion B 6.~~

~~**Statement:** Capacity Benefit Margin (CBM) is better integrated in marketing functions and is not a reliability function. In the NERC TOP-002 Operations Planning Standard, Requirement R1 specifies that the Transmission Operator shall have an Operating Planning Analysis that represents projected System conditions to assess planned operation for the next day that do not exceed Facility Ratings or Stability Limits for anticipated normal and contingency events. Further, the CBM standard is redundant to the TOP-002 R1 where the marketer would schedule their transmission reserve within the limits established by the Transmission Operator. The Transmission Operator ensures that the established reserve along with other identified schedules are modeled to anticipate next-day conditions and remain within established operating limits.~~

~~In addition, this Standard is not necessary for the support of BES reliability as evidenced by the fact that of the entities that once used CBM, many dropped it when it became effective due to the unnecessary burdens it placed on the entities.~~

~~**Conclusion:** The requirements above relate to commercial and market issues regulated under OATT.~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

~~Furthermore, they provide little protection to the BES and unnecessary as part of NERC Reliability Standards. Requirements 1 through 12 and associated subrequirements should be removed from Reliability Standard MOD-004-1.~~

NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4

R9.1 Administrative elements:

R9.1.1 Definitions of key terms used in the agreement.

R9.1.2 Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3 A requirement to review the agreement(s) at least every three years.

R9.1.4 A dispute resolution mechanism.

Criterion B 1~~, 3, 5, 6~~.

Statement: These requirements of NUC-001-2 do not address reliability, rather they address administrative and commercial terms of an agreement. Given there is no clear nexus between these requirements and reliability, they should be retired.

Conclusion: Since these requirements are purely administrative in nature, provide for a periodic update and commercial terms of the agreement, they provide little protection to the BES. Requirement 9.1 and associated sub-requirements~~subrequirements~~ should be removed from Reliability Standard NUC-001-2.

***PRC-008-0 R1; *PRC-008-0 R2; *PRC-009-0 R1; *PRC-009-0 R1.1; *PRC-009-0 R1.2; *PRC-009-0 R1.3; *PRC-009-0 R1.4; *PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2.**

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
PRC-008-0 R1 The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance. PRC-008-0 R2 The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days). PRC-009-0 R1 The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to: PRC-009-0 R1.1 A description of the event including initiating conditions. PRC-009-0 R1.2 A review of the UFLS set points and tripping times. PRC-009-0 R1.3 A simulation of the event. PRC-009-0 R1.4 A summary of the findings. PRC-009-0 R2 The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

PRC-010-0 R2 The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

PRC-022-1 R2 Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

Criterion B 1 and 2~~4, 9~~.

Statement: Under Standards Development Project 2007-17 Protection System Maintenance, which recently passed on August 27, 2012, PRC-008-0 is scheduled to be retired~~Since UVLS~~ and replaced with PRC-005-2. PRC-005-2 will likely be presented to the NERC Board of Trustees in November for approval~~UFLS information is being collected under event analysis~~, and, thus, PRC-008-0 is only presented here for informational purposes. In Order No. 763 at Paragraph 103 the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, ~~also~~ PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Thus, PRC-009-0 is presented here for informational purposes only.

Conversely, PRC-010-0 R2 and PRC-022-1 R2 are not scheduled to be retired and are purely administrative and data collection~~, the above~~ requirements that are better and more appropriately handled via spot checks/compliance audit request for evidence and the applicable RSAW.~~add little to reliability.~~

Conclusion: Since PRC-~~008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-~~010-0 R2 and~~;~~ PRC-022-1 R2 provide~~provides~~ little protection to the BES and better handled via the compliance and monitoring program~~under event analysis and lessons learned papers, it should be removed~~.

***TOP-001-1a R3**

Formatted: Tab stops: 0.5", Left

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information
Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions. Criterion B 7. **Statement:** Although there is redundancy between TOP-001-1a R3 and ~~is redundant with~~ IRO-001-1a R8 related to Reliability Coordinators, this redundancy was addressed in Standards Development Project~~. NOTE: per project~~ 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces~~), this requirement was removed from~~ TOP-001-1a R3 and ~~and proposed to be replaced by IRO-001-3, R2, R3, R4.~~ ~~**IRO-001-1a R8**~~ reads: Each~~Transmission Operators,~~ Balancing Authority~~Authorities~~, Generator Operator, Distribution Provider, and ~~Operators, Transmission Service Providers,~~ Load-Serving Entity~~Entities, and Purchasing-Selling Entities~~ shall comply with each Reliability Directive issued and identified as such by its Transmission Operator(s),~~Reliability Coordinator directives~~ unless such action~~actions~~ would violate safety, equipment, ~~or~~ regulatory, or statutory requirements. TOP-001-2 has been approved by ~~Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of~~ the NERC Board of Trustees and will be filed with~~inability to perform~~ the Commission for approval; therefore, TOP-001-1a R3 is presented for informational purposes only. ~~directive so that the Reliability Coordinator may implement alternate remedial actions.~~

Formatted: Font: Not Bold

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: 0.5", Left

Formatted: Right: 0", Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: 0.5", Left

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

~~*The next proposed version of IRO-001 for this requirement also reads the same. As is apparent from a comparison of the two requirements, there is no need for TOP-001-1a R3 which is duplicative of IRO-001-1a R8. Also, in the next proposed version of TOP-001, Reliability Coordinator has been deleted from this requirement.~~

~~**Conclusion:** Requirement 3 is redundant to Reliability Standard IRO-001-1a R8 and should be removed from Reliability Standard TOP-001-1a.~~

TOP-005-2a R1

As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."

Criterion B 3.

Statement:

TOP-005-2a R1 is better suited for ROP than reliability requirement. A review of Standards Development Project 2007-03 Real-time Transmission Operations indicates it proposes R1 of TOP-005-1 to be retired. As stated above in the context of TOP-001, this project was approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-005-2a R1 is presented for informational purposes only.

Conclusion: Since TOP-005-2a R1 provides little protection to the BES and is purely documentation in nature, it should be removed.

VAR-001-2 R5

Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

Formatted: Font: Bold

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Tab stops: 0.5", Left

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

Criterion B 7.

Statement: VAR-001-2 R5 is redundant with FERC's pro forma open access transmission tariff (OATT) Specifically, the requirement provides for the PSE and LSE to arrange for reactive resources to satisfy the reactive requirements of the Transmission Service Provider, which is already required under Schedule No. 2 of the OATT.

Conclusion: Since VAR-001-2 R5 is redundant with requirements already under FERC's OATT, and, thus, it should be removed.

~~**VAR-002-WECC-1 R2; VAR-501-WECC-1 R2**~~

~~VAR-002-WECC-1 R2 Generator Operators and Transmission Operators shall have documentation identifying the number of hours excluded for each requirement R1.1 through R1.10.~~

~~VAR-501-WECC-1 R2 Generator Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.12.~~

~~Criterion B 3 and 4.~~

~~**Statement:** Communication of the status of AVR and PSS with the Transmission Operator may impact reliability, but not documenting or reporting out of this information to a Regional Entity. If the Regional Entity desires to review or track the AVR and PSS hours, such information should be collected via vehicles other than the Reliability Standards, such as Compliance Audits, Spot Checks and other compliance monitoring procedures.~~

~~**Conclusion:** For regulatory efficiency and since the requirements are purely documentation and reporting activities, Requirement 2 in Regional Reliability Standards VAR-002-WECC-1 and VAR-501-WECC-1 should be removed from the Standards.~~

Formatted: Font: (Default) Calibri, Font color: Black

SAR Information

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☒	Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of responsible entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☒	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☒	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☒	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.

Formatted: Font: (Default) Calibri, Font color: Black

Reliability Functions		
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☒	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles		
Applicable Reliability Principles (Check all that apply).		
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.	
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.	
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.	
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.	
☒	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.	
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.	
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.	
Does the proposed Standard comply with all of the following Market Interface Principles?		Enter (yes/no)
	1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes

Formatted: Font: (Default) Calibri, Font color: Black

Reliability and Market Interface Principles	
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation

Related SARs	
SAR ID	Explanation

Formatted: Font: (Default) Calibri, Font color: Black

Regional Variances	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	

Formatted: Font: (Default) Calibri, Font color: Black

P81 Project Technical White Paper

October 23, 2012

Table of Contents

P81 Project Technical White Paper

October 23, 2012

I. Introduction

On March 15, 2012, the Federal Energy Regulatory Commission ("FERC" or Commission") issued an order[1] on the North American Electric Reliability Corporation's ("NERC") Find, Fix and Track ("FFT") process that stated in paragraph 81 ("P81"):

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the [Electric Reliability Organization] ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

A. Consensus Process

In response to P81 and the Commission's request for comments to be coordinated,[2] during June and July 2012, various industry stakeholders, Trade Associations,[3] staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. Specifically, the three parties (industry stakeholders/Trade Associations, staff from NERC, and staff from the NERC Regions) used the following

[1] *North American Electric Reliability Corporation,* 138 FERC ¶ 61,193 at P 81 (2012).

[2] In addition to addressing P81, the consensus effort was also consistent with recommendation #4 set forth in *NERC's Recommendations to Improve The Standards Development Process* at page 12 (April 2012), which states:

Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

[3] Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, and Transmission Access Policy Study Group.

conservative discipline to arrive at the proposed list of requirements to be retired: (i) the development of criteria to determine whether a Reliability Standard requirement should be retired and (ii) the application of this criteria with consultation from Subject Matter Experts ("SME"), with the understanding that if any of the three parties objected to including a requirement it would not be included in the initial phase of the P81 Project. As a result of this process, a draft Standards Authorization Request ("SAR"), including an initial suggested list of requirements for retirement, was drafted and presented to the NERC Standards Committee. Also, the SMEs consulted in this process provided the technical justifications that appear in this technical white paper.

B. Standards Committee

On July 11, 2012, the Standards Committee authorized the draft SAR to be posted for industry comment and formed an interim P81 Standards Drafting Team ("SDT") to review and respond to comments as well as finalize the SAR. The draft SAR was posted on August 3, 2012 with stakeholder comments due on or before September 4, 2012. Based on the stakeholder comments received, the SDT finalized the SAR, including the criteria and the initial list of Reliability Standard requirements proposed for retirement. On September 28, 2012, the Standards Committee Executive Committee authorized: (a) waiving the 30 day initial comment period and (b) posting the SAR and list of requirements proposed for retirement in the initial phase for a 45-day formal comment period with the formation of a ballot pool during the first 30 days and an initial ballot during the last 10 days of that 45-day comment period.[4]

The purpose of this technical white paper is to set forth the background and technical justification for each of the Reliability Standard requirements proposed for retirement. Stakeholders are requested to review this technical white paper and provide the SDT any: (1) supplemental, additional technical justifications for a requirement(s) and/or (2) concerns with the technical justifications for a requirement(s).

[4] The following requirements that were presented in the draft SAR were already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the Board in November), and, thus, are presented in this technical white paper in Section V for informational purposes only: COM-001-1.1 R6; EOP-009-0 R2; FAC-008-1 R1.3.5; PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; TOP-001-1a R3; and TOP-005-2a R1. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the Board of Trustees for retirement or filed with the Commission or Canadian governmental authorities as part of the P81 Project. Those requirements that were not part of the draft SAR, but were added based on stakeholder comments are denoted by a "**" throughout this technical white paper. More detail on each of these requirements is provided below.

II. Executive Summary

The SDT developed a set of three criteria and used them to identify requirements that could be eligible for retirement. A summary of the criteria are as follows:

A. Criterion A (Overarching Criterion): little, if any, benefit or protection to the reliable operation of the BES

B. Criteria B (Identifying Criteria)
   - B1. Administrative
   - B2. Data Collection/Data Retention
   - B3. Documentation
   - B4. Reporting
   - B5. Periodic Updates
   - B6. Commercial or Business Practice
   - B7. Redundant

C. Criteria C (Additional data and reference points)
   - C1. Part of a FFT filing
   - C2. Being reviewed in an ongoing Standards Development Project
   - C3. Violation Risk Factor ("VRF") of the requirement
   - C4. Tier in the 2013 Actively Monitored List ("AML")
   - C5. Negative impact on NERC's reliability principles
   - C6. Negative impact on the defense in depth protection of the BES
   - C7. Promotion of results or performance based Reliability Standards

Specifically, for a requirement to be proposed for retirement, it must satisfy both, Criterion A and at least one of the Criteria B. Criteria C were considered as additional information to make a more informed decision.

Based on the criteria above, the SDT proposes to retire the following 38 requirements in 23 Reliability Standard versions:

- BAL-005-0.2b R2
- CIP-001-2a R4
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3
- CIP-003-3 R4.2
- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2

- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- EOP-004-1 R1
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-1 R2
- FAC-008-1 R3
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5**
- FAC-011-2 R5**
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5**

A table is included in Appendix A with the Reliability Standard requirements proposed for retirement and a cross-reference to the associated criteria.

III. Criteria

The P81 Project focuses on identifying FERC-approved Reliability Standard requirements that satisfy the criteria set forth below.[5] Specifically, for a Reliability Standard requirement to be proposed for retirement it must satisfy **both**: (i) Criterion A (the overarching criterion) and (ii) at least one of the Criteria B listed below (identifying criteria). The purpose of having these two levels of criteria was to confine the review and consideration of requirements to only those requirements that clearly need not be included in the mandatory Reliability Standards. Also, Criteria A and B were designed

[5] The scope of future phases of the P81 Project has not yet been determined. When the scope is considered, the criteria set forth herein may be a useful guide to appropriate criteria for those phases.

so there would be no rewriting or consolidation of requirements, and the technical merits of retiring the requirements did not require significant research and vetting. In addition, for each Reliability Standard requirement proposed for retirement, the data and reference points set forth below in Criteria C were considered to make a more informed decision on whether to proceed with retirement. Lastly, for each requirement proposed for retirement, any increase to the efficiency of the ERO compliance program is addressed.

Criterion A (Overarching Criterion)
The Reliability Standard requirement requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Section 215(a) (4) of the United States Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

Criteria B (Identifying Criteria)
B1. Administrative
The Reliability Standard requirement requires responsible entities ("entities") to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

This criterion is designed to identify requirements that can be removed with little effect on reliability and whose removal will result in an increase in the efficiency of the ERO compliance program. Administrative functions may include a task that is or is not related to developing procedures or plans, such as establishing communication contacts. Thus, for certain requirements, Criterion B1 is closely related to Criteria B2, B3 and B4. Strictly administrative functions do not inherently negatively impact reliability directly and, where possible, should be eliminated for purposes of efficiency and to allow the ERO and entities to appropriately allocate resources.

B2. Data Collection/Data Retention
These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

This criterion is designed to identify requirements that can be removed with little effect on reliability. The collection and/or retention of data do not necessarily have a reliability benefit and yet are often required to demonstrate compliance. Where data collection and/or data retention is unnecessary for reliability purposes, such requirements should be eliminated in order to increase the efficiency of the ERO compliance program.

B3. Documentation
The Reliability Standard requirement requires responsible entities to develop a document (*e.g.*, plan, policy or procedure) which is not necessary to protect BES reliability.

This criterion is designed to identify requirements that require the development of a document that is unrelated to reliability or has no performance or results-based function. In other words, the document is required, but no execution of a reliability activity or task is associated with or required by the document.

B4. Reporting
The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there would be little reliability impact.

B5. Periodic Updates
The Reliability Standard requirement requires responsible entities to periodically update (*e.g.*, annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

This criterion is designed to identify requirements that impose an updating requirement that is out of sync with the actual operations of the BES, unnecessary or duplicative.

B6. Commercial or Business Practice
The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

This criterion is designed to identify those requirements that require: (i) implementing a best or outdated business practice or (ii) implicating the exchange of or debate on commercially sensitive information while doing little, if anything, to promote the reliable operation of the BES.

B7. Redundant
The Reliability Standard requirement is redundant with (i) another FERC-approved Reliability Standard requirement(s); (ii) the ERO compliance and monitoring program or (iii) a governmental regulation (*e.g.*, Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

This criterion is designed to identify requirements that are redundant with other requirements and are, therefore, unnecessary. Unlike the other criteria listed in Criterion B, in the case of redundancy, the task or activity itself may contribute to a reliable BES, but it is not necessary to have two duplicative requirements on the same or similar task or activity. Such requirements can be removed with little or no effect on reliability and removal will result in an increase in efficiency of the ERO compliance program.

Criteria C (Additional data and reference points)
In those instances where there is a need for additional information to assist in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B, the following data and reference points shall be considered to make a more informed decision:

C1. Was the Reliability Standard requirement part of a FFT filing?

The application of this criterion involves determining whether the requirement was included in a FFT filing.

C2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?

The application of this criterion involves determining whether the requirement proposed for retirement is part of an active on-going Standards Development Project, with a consideration of the point in the process that Project is at. If the requirement has been passed by the stakeholders and is scheduled to be presented to the NERC Board of Trustees, in most cases it will not be included in the P81 project to promote regulatory efficiency. The exception would be a requirement, such as the Critical Information Protection ("CIP") requirements for Version 3 and 4, that is not due to be retired for an extended period of time; or, other requirements that based on the specific facts and circumstances of that requirement indicate it should be retired via the P81 Project first rather than waiting for another Standards Development Project to retire it, particularly as a way to increase the efficiencies of the ERO compliance program. Also, for informational purposes, whether the requirement is included in a future or pending Standards Development Project will be identified and discussed.

C3. What is the VRF of the Reliability Standard requirement?

The application of this criterion involves identifying the VRF of the requirement proposed for retirement, with particular consideration of any requirement that has been assigned as having a Medium or High VRF. Also, the fact that a requirement has a Lower VRF is not dispositive that it qualifies for retirement. In this regard, Criterion C3 is considered in light of Criterion C5 (Reliability Principles) and C6 (Defense in Depth) to ensure that no reliability gap would be created by the retirement of the Lower VRF requirement. For example, no requirement, including a Lower VRF requirement, should be retired if its retirement harms the effectiveness of a larger scheme of requirements that are purposely designed to protect the reliable operation of the BES.

C4. In which tier of the 2013 AML does the Reliability Standard requirement fall?

The application of this criterion involves identifying whether the requirement proposed for retirement is on the 2013 AML, with particular consideration for any requirement in the first tier of the 2013 AML.

C5. Is there a possible negative impact on NERC's published and posted reliability principles?

The application of this criterion involves consideration of the eight following reliability principles published on the NERC webpage.

> **Reliability Principles**
> NERC Reliability Standards are based on certain reliability principles that define the foundation of reliability for North American bulk power systems. Each reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of reliability of the North American bulk power systems. Each reliability standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.
>
> Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
>
> Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
>
> Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
>
> Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

Principle 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

Principle 7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks. (footnote omitted).

C6. Is there any negative impact on the defense in depth protection of the BES?

The application of this criterion considers whether the requirement proposed for retirement is part of a defense in depth protection strategy. In order words, the assessment is to verify whether other requirements rely on the requirement proposed for retirement to protect the BES.

C7. Does the retirement promote results or performance based Reliability Standards?

The application of this criterion considers whether the requirement, if retired, will promote the initiative to implement results- and/or performance-based Reliability Standards.

IV. The Initial Phase Reliability Standards Requirements Proposed for Retirement

The following lists the requirements proposed for retirement with details of the assessment resulting from the applicability of the criteria above.

BAL-005-0.2b R2 – Automatic Generation Control

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

Background/Commission Directives

BAL-005-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[6] Also, the Commission accepted an errata filing to BAL-005-0.1b, which replaced Appendix 1 with a corrected version of a Commission-approved interpretation, and made an internal reference correction in the interpretation, thus resulting in BAL-005-0.2b.[7]

In Order No. 693 at paragraph 387, the Commission stated that:

> The goal of this Reliability Standard is to maintain Interconnection frequency by requiring that all generation, transmission, and customer load be within the metered boundaries of a balancing authority area, and establishing the functional requirements for the balancing authority's regulation service, including its calculation of ACE.

At paragraph 396, the Commission stated:

> On this issue, the Commission directs the ERO to modify BAL-005-0 through the Reliability Standards development process to develop a process to calculate the minimum regulating reserve for a balancing authority, taking into account expected load and generation variation and transactions being ramped into or out of the balancing authority.

This Commission directive is unaffected by the proposed retirement of BAL-005-0.2b R2.

Additionally, when adjusting the VRF for the previous version, BAL-005-0.1b R2, from Lower to High, the Commission stated that:[8]

> While theoretically, CPS can be met without the use of AGC, for example, when the AGC system is malfunctioning, the Commission believes, in practice, that AGC is the most dependable and effective means for multiple balancing authorities in an Interconnection to collectively meet CPS requirements in tandem while minimizing assistance from each other in this regard. Human reaction is neither fast enough nor dependable enough in this repetitive task to provide the immediate and continuous support to correct for Interconnection frequency drift. Further, the failure to use AGC presents a higher risk that immediate load shedding will need to be implemented after the sudden loss of generation or an unforeseen

[6] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[7] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Errata Changes to Seven Reliability Standards, Docket No. RD12-4-000 (September 13, 2012).

[8] *North American Electric Reliability Corporation*, 121 FERC ¶ 61,179 at P 50 (2007).

> significant load increase and, thus, the failure to use AGC subjects the Bulk-Power System to a higher risk of instability.

However, the fact that the VRF for BAL-005-0.2b R2 is High is not indicative of its actual impact on the BES as explained in further detail below. Also, no Commission directive is impacted by BAL-005-0.2b R2.

Technical Justification

The stated reliability purpose of BAL-005-0.2b is to establish requirements for Balancing Authority Automatic Generation Control ("AGC") necessary to calculate Area Control Error ("ACE") and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved. The reliability purpose and objectives of BAL-005-0.2b are unaffected by the proposed retirement of R2.

A Balancing Authority must use AGC to control its Regulating Reserves to meet the Control Performance Standards ("CPS") as set forth in BAL-001-0.1a R1 and R2. Although for a short period of time (as the Commission stated during an AGC malfunction) a Balancing Authority may be able to meet its CPS obligations without AGC, it cannot do so for any extended period of time, and, therefore, Balancing Authorities must use AGC to control its Regulating Reserves to satisfy its obligations under BAL-001-0.1a R1 and R2. Given this fact, it is redundant to also have BAL-005-0.2b R2 set forth the following statement: "Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard." (Criterion B7). It is the duplicative nature of having two requirements requiring the same activity that does little, if anything, to benefit or protect reliable operation of the BES. (Criterion A). In other words, without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a R1 and R2.

Also, the retirement of BAL-005-0.2b R2 would increase the efficiency of the ERO compliance program because NERC and the Regional Entities would be able to focus their time and resources on monitoring compliance on BAL-001-0.1a R1 and R2, which are results-based requirements, versus monitoring compliance with both BAL-001-0.1a R1 and R2 as well as the static statement in BAL-005-0.2b R2. Therefore, retiring BAL-005-0.2b R2 will provide for increased efficiencies in the ERO compliance program.

Criterion A

Without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a R1 and R2. Having two requirements requiring a Balancing Authority to conduct the same activity or task does little, if anything, to benefit or protect the reliable operation of the BES because it is duplicative.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. BAL-005-0.2b R2 has not been part of a FFT filing.

2. BAL-005-0.2b R2 is currently scheduled to be included in Standards Development Project 2010-14.2, which is Phase II of Balancing Authority Reliability-based Controls: Time Error, AGC, and Inadvertent. Given that Project 2010-14.2 is currently not an active Standards Development Project, it remains appropriate to retire BAL-005-0.2b R2 via the P81 Project.

3. The VRF for BAL-005-0.2b R2 is High. Given the redundant nature of BAL-005-0.2b R2, the High VRF is not dispositive of whether or not it should be retired since BAL-001-0.1a R1 and R2 accomplishes the important reliability requirement of Balancing Authorities maintaining Regulating Reserves that can be controlled by AGC to satisfy CPS.

4. BAL-005-0.2b R2 is not part of the 2013 AML.

5. The redundant nature of BAL-005-0.2b R2 with BAL-001-0.1a R1 and R2 also indicates that the retirement of BAL-005-0.2b R2 does not pose a negative impact to NERC's published and posted reliability principles. The two reliability principles applicable to BAL-005-0.2b R2 are the following:

    Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

    Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement of BAL-005-0.2b R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. As discussed above, given that BAL-001-0.1a R1 and R2 already require that AGC be used to control Regulating Reserves, there is no risk or gap to reliability resulting from the retirement of BAL-005-0.2b R2.

7. Retirement of BAL-005-0.2b R2 promotes a results-based approach, because it is retiring a static requirement while BAL-001.1a R1 and R2, which are more dynamic and results-based requirements, will remain in effect.

Accordingly, for the above reasons, it is appropriate to retire BAL-005-0.2b R2.

CIP-001-2a R4 Sabotage Reporting

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

Background/Commission Directives

CIP-001-1 was filed for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[9] CIP-001-1a was filed for Commission approval on April 21, 2010 in Docket No. RD10-11-000, and was approved by an unpublished letter order on February 2, 2011.[10]

CIP-001-2a was filed for Commission approval as a Regional Variance for the ERCOT Region, containing an interpretation of CIP-001-1, on June 21, 2011 in Docket No. RD11-6-000 and was approved by unpublished letter order on August 2, 2011.[11]

In Order No. 693 at paragraph 460, the Commission stated:

> For these reasons, the Commission remains concerned that a wider application of CIP-001-1 may be appropriate for Bulk-Power System reliability. Balancing these concerns with our earlier discussion of the applicability of Reliability Standards to smaller entities, we will not direct the ERO to make any specific modification to CIP-001-1 to address applicability. However, we direct the ERO, as part of its Work Plan, to consider in the Reliability Standards development process, possible revisions to CIP-001-1 that address our concerns regarding the need for wider application of the Reliability Standard. Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.

In Order No. 693 at paragraphs 445 and 467 through 470, the Commission stated that:

> The goal of CIP-001-1 is to ensure that operating entities recognize sabotage events and inform appropriate authorities and each other to

[9] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[10] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-001-1 —Cyber Security— Sabotage Reporting, Requirement R2, Docket No. RD10-11-000 (February 2, 2011).
[11] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of the Reliability Standard CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity, Docket No. RD11-6-000 (August 2, 2011).

properly respond to the sabotage to minimize the impact on the Bulk-Power System. The Reliability Standard requires that each reliability coordinator, balancing authority, transmission operator, generation operator and LSE have procedures for recognizing and for making operating personnel aware of sabotage events, and communicating information concerning sabotage events to appropriate "parties" in the Interconnection.

* * *

CIP-001-1, Requirement R4, requires that each applicable entity establish communications contacts, as applicable, with the local FBI or Royal Canadian Mounted Police officials and develop reporting procedures as appropriate to its circumstances. The Commission in the NOPR expressed concern that the Reliability Standard does not require an applicable entity to actually contact the appropriate governmental or regulatory body in the event of sabotage. Therefore, the Commission proposed that NERC modify the Reliability Standard to require an applicable entity to "contact appropriate federal authorities, such as the Department of Homeland Security, in the event of sabotage within a specified period of time."

As mentioned above, NERC and others object to the wording of the proposed directive as overly prescriptive and note that the reference to "appropriate federal authorities" fails to recognize the international application of the Reliability Standard. The example of the Department of Homeland Security as an "appropriate federal authority" was not intended to be an exclusive designation. Nonetheless, the Commission agrees that a reference to "federal authorities" could create confusion. Accordingly, we modify the direction in the NOPR and now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event. The ERO's Reliability Standards development process should develop the language to implement this directive.

* * *

Thus, the Commission directs the ERO to modify CIP-001-1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time, even if it is a preliminary report. The ERO, through its Reliability Standards development process, is directed to determine the proper reporting period. In doing so, the ERO should consider suggestions raised by commenters such as FirstEnergy and Xcel to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage, and APPA's concerns regarding events at unstaffed or remote

> facilities, and triggering events occurring outside staffed hours at small entities. (Footnotes omitted).

The Commission's suggestion to modify CIP-001-1 to require an applicable entity to contact appropriate federal authorities, such as the Department of Homeland Security, is being considered in Standards Development Project 2009-01 (EOP-004-2). CIP-001-2a R4 is proposed for retirement because it does not require an action when sabotage is suspected or actually occurs, rather that action is addressed via CIP-001-2a R2.

Technical Justification

The practices and procedures set forth in CIP-001-2a R2 provides the results-based foundation for contacting communication of information concerning sabotage events to appropriate parties in the Interconnection, including when necessary, the FBI or RCMP, when there is an event of suspected or actual sabotage, while the task in R4 does little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A). Consistent with CIP-001-2a R1 (identification of sabotage), R2 (communication of sabotage) and R3 (reporting of sabotage),[12] a responsible entity generally contacts local law enforcement authorities when there is any suspicion that sabotage has occurred at a BES facility. The entity's corporate security and site personnel will consult with local law enforcement to assess the situation and facts to determine whether a suspected or actual act of sabotage has occurred. If they find a suspected or actual act of sabotage has occurred, the FBI or RCMP, as appropriate, will be contacted in accordance with R2.[13] Thus, pursuant to the different steps and actions in R1 through R3, when there is an instance of sabotage that warrants contacting the FBI or RCMP or any other federal/national governmental authority, the responsible entities will contact them. Conversely, CIP-001-2a R4 does not require that the FBI or RCMP be contacted when an act of suspected or actual sabotage has occurred; instead, R4 only requires that the entity establish communication contacts with these agencies, as appropriate, and "develop reporting procedures. . . ." While the development of reporting procedures in R4 is generic, the procedures and processes associated with R1, R2, and R3 are specific to the steps of identifying, communicating and reporting issues related to sabotage. This view was confirmed in the interpretation of R2 that states:

> . . . the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information.

[12] "**R2.** Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection."

[13] In addition, the requirement, as written, does not reflect current reporting and investigation procedures in some of the Canadian Provinces as protocol for sabotage reporting and investigation varies in each Canadian Province. For example, in the Provinces of Ontario and Quebec, the reports are given to local police (municipal/provincial) and not to the RCMP as the standard specifies. The fact is that the RCMP does not perform Provincial level law enforcement in the Provinces of Ontario and Quebec.

Consequently, the R4 requirement to establish communication contacts and develop reporting procedures does not support reliability, and, instead, is an administrative, documentation and data collection task requirement (Criteria B1, B2 and B3). Also, in the overall context of CIP-001-2a R1 through R3, which already require sabotage related procedures and guidelines, the tasks in R4 are unnecessary and needlessly burdensome. Furthermore, corporate security departments that are involved in the investigation of sabotage related events are well aware of how to contact the FBI and RCMP, as applicable, and, in fact, some corporate security employees to have a law enforcement background, including past positions in federal agencies such as the Secret Service. To have these security professionals establish contacts with agencies they are readily familiar with and to generic develop reporting procedures that do not require action is unnecessarily burdensome. The administrative aspect of R4 is further illuminated when compared to the more results-based activities in CIP-001-2a R1 through R3, which are the requirements that serve reliability by requiring action when suspected or actual sabotage occurs. Accordingly, CIP-001-2a R1 through R3 serve the results-based reliability function, while R4 is a static, administrative requirement that has no direct or clear nexus to protecting BES reliability.

Also, the retirement of CIP-001-2a R4 should increase the efficiencies of the ERO compliance program, because ERO and Regional Entity time and resources would be able to focus more attention, if needed, on monitoring compliance with CIP-001-2a R1 through R3.

Criterion A

CIP-001-2a R2 provides the results-based foundation for contacting communication of information concerning sabotage events to appropriate parties in the Interconnection, including when necessary, the FBI or RCMP, when there is an event of suspected or actual sabotage, while the task in R4 does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)
- Criterion B3 (Documentation)

Criteria C

1. CIP-001-2a R4 has been part of a FFT filing.[14]

[14] NERC FFT Informational Filing, Docket No. RC12-15-000 (August 31, 2012); NERC FFT Informational Filing, Docket No. RC12-13-000 (June 29, 2012); NERC FFT Informational Filing, Docket No. RC12-11-000 (April 30, 2012); NERC FFT Informational Filing, Docket No. RC12-6-000 (December 30, 2011); NERC FFT Informational Filing, Docket No. RC12-2-000 (November 30, 2011); NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011); NERC FFT Informational Filing, Docket No. RC11-6-000 (September 30, 2011).

2. CIP-001-2a R4 is part of an on-going Standards Development Project 2009-01 (EOP 004-2). At this time, EOP-004-2 has not been approved by stakeholders and the NERC Board of Trustees, and, therefore, it is appropriate to retain CIP-001-2a R4 within the scope of P81. However, if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 Project and may include CIP-001-2a R4 for informational purposes only.

3. CIP-001-2a R4 has a Medium VRF. All of CIP-001-2a has a Medium VRF, thus the fact that R4 is a Medium VRF is not dispositive of whether it should be retired.

4. CIP-001-2a R4 is in the second tier of the AML. Similar to the VRF, having CIP-001-2a R4 in the second tier of the AML is not dispositive of whether it should be retired, particularly when considered with the fact that R2 and R3, the more results-based requirements, are in the first tier.

5. Given its lack of requiring a reliability based action, the retirement of CIP-001-2a R4 does not negatively impact NERC's published and posted reliability principles. The only principles applicable to CIP-001-2a R4 appear to be the following:

   Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

   Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks.

6. The retirement of CIP-001-2a R4 does not impact a defense in depth strategy between multiple requirements. CIP-001-2a R1 through R3 provide the foundation for the identification, communication and reporting of suspected and actual sabotage, while R4 is an administrative task of establishing contacts and developing generic reporting procedures. Therefore, there is no reliability risk or gap that will result from the retirement of CIP-001-2a R4.

7. As mentioned above, CIP-001-2a R4 is not a results-based requirement.

Accordingly, for the above reasons, it is appropriate to retire CIP-001-2a R4.

CIP-003-3, -4 R1.2 – Cyber Security – Security Management Controls

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[15] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[16] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[17] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[18]

In Order No. 706 at paragraph 342 the Commission stated that:

> Reliability Standard CIP-003-1 seeks to ensure that each responsible entity has minimum security management controls in place to protect the critical cyber assets identified pursuant to CIP-002-1. To achieve this goal, a responsible entity must develop a cyber security policy that represents management's commitment and ability to secure its critical cyber assets. It also must designate a senior manager to direct the cyber security program and to approve any exception to the policy.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R1.2 does not impact a Commission directive.

Technical Justification

The importance of the cyber security policy as representing management's commitment and ability to secure critical cyber assets is overshadowed by the rigorous and specific training, procedural and process related requirements of the CIP Standards. These trainings, procedures and processes render having the cyber security policy readily available an unnecessary requirement. In other words, whether CIP personnel are completing a typical CIP requirement cyber security task or responding to an immediate situation, they will act via their specific training, processes and procedures and not the overarching cyber security policy. Consequently, the cyber security policy's generalized guidance on compliance with the CIP requirements is not a document that adds value to personnel protecting the BES from a cyber attack on a day-to-day basis.

---

[15] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[16] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

[17] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

[18] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

Furthermore, to implement CIP-003-3, -4 R1.2 entities have undertaken a variety of administrative solutions including kiosks dedicated to computers with the cyber security policy, posting the policy on the company intranet, having copies available in work stations, at common area desks in generating stations and substations, etc. Therefore, although the cyber security policy is readily available for all personnel who have access to, or are responsible for, Critical Cyber Assets, these personnel are specifically and appropriately focused on implementing the procedures and processes required by CIP Reliability Standards such as CIP-007-3 R1, which states as follows:

> Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

Generally the cyber security policy will cite CIP-007-3 R1 as a requirement, and may refer to procedures related to CIP-007-3 R1, but will not have, nor is it required to have, the detail necessary to implement CIP-007-3 R1. In some larger companies, it is also common to have specific procedures on how to accomplish requirements such as CIP-007-3 R1 in a control center versus a generating plant or substation, and it may be different CIP personnel implementing these procedures in locations many hundreds of miles, states or Interconnections away from each other. The value of a more general cyber security policy to these individuals is minimal, at best, and, therefore, does not support reliability. Also, making it readily available at all office locations is an unnecessarily burdensome administrative task.

Moreover, to place every procedure and process to comply with CIP in the cyber security policy is also not practical or effective, because such a large policy will only distract from CIP personnel being able to specifically focus on the task before them. As already stated, there are likely some differences between implementing a requirement like CIP-007-1 R1 in a control center that may be located in one state and for generators located several states and hundreds of miles away. Thus, making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES (Criteria A and B1).

In this context, also consider the inefficiencies CIP-003-3, -4 R1.2 may be causing the ERO compliance program. In companies with hundreds of personnel who have access to, or are responsible for, Critical Cyber Assets in multiple states and Interconnections, the ERO may expend a significant amount of time and resources to monitor compliance with CIP-003-3, -4 R1.2 via a review of kiosks, intranet sites, office cubicles, desks, etc in

multiple locations. Accordingly, considerable efficiency gains will be obtained for the ERO's compliance program if CIP-003-3, -4 R1.2 is retired.

Criterion A
Making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. CIP-003-3, -4 R1.2 has been part of a FFT filing.[19]

2. As is the case with all the CIP requirements (other than CIP-001-2a R4) proposed for retirement in this technical paper, CIP-003-3, -4 R1.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security) ("CIP V5"). The P81 SDT has coordinated its efforts with the chair of Project 2008-06. There is no conflict between CIP requirements proposed in this technical white paper for retirement and the direction of Project 2008-06. The CIP V5 requirements are not Board of Trustee or Commission approved, and, even if they were, the effective date of CIP V5 is unknown and likely at least a year, maybe more, into the future. Thus, unlike the other requirements presented here for informational purposes, it is appropriate to maintain all the CIP requirements discussed in this technical paper within the scope of the P81 Project to secure the efficiency gains resulting to the ERO compliance program from their retirement.

3. CIP-003-3, -4 R4.2 has a Lower VRF. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-003-3,-4 R1.2 is in the second tier of the AML. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given its administrative nature, CIP-003-3, -4 R1.2 does not negatively impact NERC's published and posted reliability principles. The two reliability principles that appear applicable to CIP-003-3, -4 R1.2 are the following:

   Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

[19] NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks.

As stated above, other CIP requirements are replete with the requirements that CIP personnel implement to protect the BES from cyber attacks.

6. Retiring CIP-003-3, -4 R1.2 does not negatively impact defense in depth because no other requirement depends on the cyber security policy being readily available. Therefore, the removal of CIP-003,-3,-4 R1.2 cannot have a negative impact on defense in depth.

7. Retirement of CIP-003-3, -4 R1.2 promotes a results-based approach because the requirement is mechanistic and administrative, and does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R1.2.

CIP-003-3, -4 R3, R3.1, R3.2, R3.3 – Cyber Security – Security Management Controls

R3. Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[20] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-

[20] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

000 and was approved on September 30, 2009.[21] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[22] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[23]

In Order No. 706 at paragraphs 373 and 376 the Commission stated that:

> Requirement R3 provides that a responsible entity must document exceptions to its policy with documentation and senior management approval. The Commission is concerned that, if exceptions mount, there would come a point where the exceptions rather than the rule prevail. In such a situation, it is questionable whether the responsible entity is actually implementing a security policy. We therefore believe that the Regional Entities should perform an oversight role in providing accountability of a responsible entity that excepts itself from compliance with the provisions of its cyber security policy. Further, we believe that such oversight would impose a limited additional burden on a responsible entity because Requirement R3 currently requires documentation of exceptions.
>
> Further, the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 do not impact a Commission directive.

Technical Justification

CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 (CIP exception requirements) have proven not to be useful and have been subject to misinterpretation. For instance, although the CIP exception requirements have not been available for use to exempt an entity from compliance with any requirement of any Reliability Standard, based on questions received by NERC CIP Staff, entities may be interpreting the CIP exception requirements to allow for such an exemption. The CIP exception requirements only apply to

[21] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

[22] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

[23] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

exceptions to internal corporate policy, and only in cases where the policy exceeds a Reliability Standard requirement or addresses an issue that is not covered in a Reliability Standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of eight characters in length, and be changed every 30 days, which is over and above what is required in CIP-007-3 R5.3, the CIP exception requirements could be invoked for internal governance purposes to lessen the corporate requirement back to the password requirements in CIP-007-3 R5.3, but under no circumstances do the CIP exception requirements authorize the implementation of security measures less than what is required in CIP-007-3 R5.3.

The retirement of the CIP exception requirements would not impact an entity's ability to maintain such an exception process within their corporate policy governance procedures, if it so desired. Consequently, the CIP exception requirements were always an internal administrative and documentation requirement that is outside the scope of the other CIP requirements (Criteria B1 and B3). In this context, the CIP exception requirements do not support the level of reliability set forth in the Reliability Standards, and are unnecessarily burdensome because they have resulted in entities implementing practices due to a misinterpretation of the requirement that has caused them to allocate time and resources to tasks that are misaligned with the requirements themselves. Unfortunately, this misunderstanding has also impacted the efficiency of the ERO compliance program because of the amount of time and resources needed to clear up the misunderstanding and coach entities on the meaning of the CIP exception requirements. These inefficiencies would be eliminated with the retirement of the CIP exception requirements. Accordingly, as explained, the CIP exception requirements are an administrative tool for internal corporate governance procedures, and, therefore, are not requirements that are necessary or directly protect the BES from a cyber attack, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A).

Criterion A
The CIP exception requirements are a tool for internal corporate governance procedures and is not a requirement directly protecting the BES from a cyber attack, and, therefore, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C

1. The CIP exception requirements have been part of a FFT filing.[24]

[24] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-6-000 (December 30, 2011).

2. The CIP exception requirements are part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between the CIP exception requirements proposed in this technical white paper for retirement and the direction of Project 2008-06.

3. The CIP exception requirements each have a Lower VRF. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. The CIP exception requirements are on the third tier of the AML. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the administrative and unnecessary nature of the CIP exception requirements in relation to protecting the BES from cyber attacks, retirement does not pose any negative impact to NERC's published and posted reliability principles, of which only Principle 8 appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. Retiring the CIP exception requirements does not negatively impact any defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of the CIP exception requirements promotes a results-based approach because the CIP exception requirements are approaches that entities may voluntarily take to handle internal corporate governance procedures, and, therefore, do not provide the foundation for performing a required reliability task.

Accordingly, for the above reasons, it is appropriate to retire the following CIP exception requirements: CIP-003-3, -4 R3, R3.1, R3.2, and R3.3.

CIP-003-3, -4 R4.2 - Cyber Security – Security Management Controls

> **R4.2.** The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[25] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-

[25] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

000 and was approved on September 30, 2009.[26] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[27] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[28] In Order No. 706, the Commission did not specifically address CIP-003-3, -4 R4.2.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R4.2 does not impact a Commission directive.

Technical Justification

The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an unnecessarily administrative and a documentation task that is redundant with CIP-003-3, -4 R4 (Criteria A, B1, B3 and B7). Specifically, CIP-003-3, -4 R4[29] already requires the classification of information associated with Critical Cyber Assets. The only difference between R4 and R4.2 is that the subjective term "based on the sensitivity" has been added, thus, making it essentially redundant. Further, CIP-003-3, -4 R4 since requires the entity to develop classifications based on a subjective understanding of sensitivity (*i.e.*, no clear connection to serving reliability), the requirement does not support reliability. In this context, classifying based on sensitivity becomes an administrative that becomes necessarily burdensome, because of all the possible ramifications "based on sensitivity" can produce, and, therefore, require SMEs to decide on and reduce to writing in a documented program. This is time and effort that could be better spent on other CIP activities that provide value to cyber security and actively protect the BES. For similar reasons, retiring CIP-003-3, -4 R4.2 and the term "based on sensitivity" would increase the efficiencies of the ERO compliance program on several levels. The ERO would not spend time and resources on reviewing whether an entity's documentation contained classifications "based on sensitivity," and, instead would be able to focus its time and resources monitoring compliance with the entity's program to identify, classify, and protect information associated with Critical Cyber Assets (R4), without any distraction on monitoring the subjective implementation of classifications based on sensitivity (R4.2).

Criterion A

The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an administrative and a documentation task that is redundant with CIP-003-3, -4 R4.

[26] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[27] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[28] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, (2012).
[29] "**R4**. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets."

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)
- Criterion B7 (Redundant)

Criteria C

1. CIP-003-3, -4 R4.2 has been part of a FFT filing.[30]

2. CIP-003-3, -4 R4.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-003-3, -4 R4.2 and the direction of Project 2008-06.

3. CIP-003-3, -4 R4.2 has a Lower VRF. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-003-3, -4 R4.2 is on the third tier of the AML. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the unnecessary and redundant nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8 which appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. Retirement of CIP-003-3, -4 R4.2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of CIP-003-3, -4 R4.2 promotes a results-based approach because retiring CIP-003-3, -4 R4.2 moves away from prescriptive, checklist of documentation approach to Reliability Standard requirements.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R4.2.

CIP-005-3a, -4a R2.6 – Cyber Security – Electronic Security Perimeter(s)

R2.6. Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen

[30] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

Background/Commission Directives

CIP-005-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[31] CIP-005-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RD09-7-000 and RM06-22-000 and was approved on September 30, 2009.[32] CIP-005-2a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by unpublished letter order on February 2, 2011.[33] CIP-005-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[34] CIP-005-3a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by an unpublished letter order on February 2, 2011.[35] CIP-005-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No. 761.[36] CIP-005-4a was filed for Commission approval as errata to the CIP Version 4 Petition on April 12, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No 761, the Final Rule on the CIP Version 4 standards.[37]

In Order 706 at paragraph 505 the Commission noted that:

> Requirement R2 of CIP-005-1 requires a responsible entity to implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-005-3, -4 R2.6 does not impact a Commission directive.

[31] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[32] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[33] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).
[34] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[35] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).
[36] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).
[37] *Id.*

Technical Justification

The implementation of an appropriate use banner ("banner") on a user's screen for all interactive access attempts into the Electronic Security Perimeter ("ESP") is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES. Specifically, the banner does not support reliability because people who intend to inappropriately use sites will simply ignore the banner. (Criterion A). The banner is also is an administrative task since it simply requires a message be displayed on an access screen. Furthermore, the implementation and administration of a non-beneficial tool, such as the banner, therefore creates a needlessly burdensome task. As mentioned, above, the ineffectiveness of the banner also indicates that it does not support reliability. (Criteria B1 and B3). In addition, banners of this type are generally considered to be a form of legal protection or mitigation of liability, rather than security protection. Furthermore, the banner does not ensure a proper or secure access point configuration which is generally the purpose of CIP-005-3a, -4a. Further, this requirement has also been the subject of numerous TFEs for devices that cannot support such a banner, and hence has diverted resources from more productive efforts. Thus, the ERO's compliance program would become more efficient if CIP-005-3a, -4a R2.6 was retired, because ERO time and resources could be reallocated to monitor compliance with the remainder of CIP-005-3a, -4a, which provides for more effective controls of electronic access at all electronic access points into the ESP.

Criterion A

The implementation of an appropriate use banner on a user's screen for all interactive access attempts into the ESP is an activity or task that does little, if anything, to benefit or protect reliable operation of the BES, because it is administrative and a static electronic message that is not an effective deterrent or control against unauthorized access.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C

1. CIP-005-3a, -4a R2.6 has been part of a FFT filing.[38]

2. CIP-005-3a, -4a R2.6 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-005-3a, -4a R2.6 and the direction of Project 2008-06.

[38] NERC FFT Informational Filing, Docket No. RC12-13-000 (June 29, 2012); NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012).

3. The VRF for CIP-005-3a, -4a R2.6 is Lower. As explained above, CIP-005-3a, -4a R2.6 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-005-3a, -4a R2.6 is on the first tier of the AML; however, given its clear ineffective nature the placement on the first tier is not dispositive of whether it should be retired.

5. Reliability principle No. 8 – "Bulk power systems shall be protected from malicious physical or cyber attacks" – is not implicated or negatively impacted by the retirement of CIP-005-3a, -4a R2.6, because it is not an effective deterrent or control to unauthorized access into an ESP.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. Furthermore, the remainder of CIP-005-3a, -4a provides for actual controls of electronic access at all electronic access points which addresses the reliability risk associated with unauthorized access into an ESP.

7. Its retirement also promotes a results-based approach because CIP-005-3a, -4a R2.6 is an ineffective administrative task, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-005-3a, -4a R2.6.

CIP-007-3, -4 R7.3 – Cyber Security – Systems Security Management

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Background/Commission Directives

CIP-007-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[39] CIP-007-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[40] CIP-007-2a was filed for Commission approval on November 17, 2009 in Docket No. RD10-3-000 and was approved on March 18, 2010.[41] CIP-007-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[42] CIP-007-4 was filed

[39] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[40] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[41] Order Approving Reliability Standard Interpretation, 130 FERC ¶ 61,184 (2010).
[42] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[43]

In Order No. 706 at paragraph 631 the Commission stated that:

> Requirement R7 of CIP-007-1 requires the responsible entity to establish formal methods, processes and procedures for disposal or redeployment of cyber assets. In the CIP NOPR, the Commission addressed the concern that solely to "erase the data," as stated several times in Requirement R7, may not be adequate because technology exists that allows retrieval of "erased" data from storage devices, and that effective protection requires discarded or redeployed assets to undergo high quality degaussing. We noted that erasure is as much a method as it is a goal, and that the requirement ultimately needs to assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. Degaussing is not the sole means for achieving this goal. The Commission therefore proposed to direct the ERO to modify Requirement R7 to clarify this point. (Footnote omitted)

This Commission directive is unaffected by the retirement of CIP-007-3,-4 R7.3 as explained below.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. [44] CIP-007-3, -4 R7.3 requires the maintaining of records for the purpose of demonstrating compliance with disposing of or redeploying of Cyber Assets in accordance with documented procedures. NERC and the Regions Entities, however, under Section 400 already have the ability to require the production of records to demonstrate compliance, thus it is unnecessary to also state the same in CIP-007-3, -4 R7.3. The maintaining of records is an administrative task, not a task directly related to the protection of the BES from a cyber attack. The maintaining of records is not a task that by itself, or in conjunction with other requirements, supports reliability. Also, the maintaining of the records becomes unnecessarily burdensome in that it requires all records be maintained, which

[43] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

[44] Section 401 of NERC's Rules of Procedure provide for collection of data and information necessary to monitor compliance outside the context of Reliability Standards:

> **Data Access** — All Bulk Power System owners, operators, and users shall provide to NERC and the applicable Regional Entity such information as is necessary to monitor compliance with the Reliability Standards. NERC and the applicable Regional Entity will define the data retention and reporting requirements in the Reliability Standards *and compliance reporting procedures.* (emphasis added).

may or may not be necessary to demonstrate compliance via the production of information under Section 400. (Criteria B1 and B2). As mentioned, CIP-007-3, -4 R7.3 does not promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A).

In contrast, the remaining substantive requirements in R7 read as follows:

> R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.
>
> R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
>
> R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

An entity's following of these requirements may help to protect BES reliability, but the retention of evidence associated with these requirements does not. Hypothetically, an entity could perform R7, R7.1 and R7.2 flawlessly and protect the BES, but not have any record of it. While this situation may impact a demonstration of compliance, the lack of records does not necessarily directly impact the reliability of the BES or protect it from a cyber attack.

Also, there are some inherent inefficiencies resulting from a small number of Reliability Standard requirements mandating the collection of data, evidence and records, while most data and information is collected for ERO compliance monitoring purposes outside the context of Reliability Standards. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A

CIP-007-3, -4 R7.3 does promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. CIP-007-3, -4 R7.3 has not been part of a FFT filing.

2. CIP-007-3, -4 R7.3 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-007-3, -4 R7.3 and the direction of Project 2008-06.

3. The VRF for CIP-007-3, -4 R7.3 is Lower. As explained above, CIP-007-3, -4 R7.3 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-007-3, -4 R7.3 is on the first tier of the AML; however, given that it is simply requiring the retention of records the fact that is on the first tier is not dispositive of whether it should be retired.

5. Given the administrative, data collection nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. The retirement does not negatively impact defense in depth because data retention in-and-of-itself is not an activity that other requirements depend on to help cover a reliability gap or risk to reliability.

7. Its retirement promotes a results-based approach because the data collection/retention does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-007-3, -4 R7.3.

EOP-004-1 R1 – Disturbance Reporting

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

Background/Commission Directives

EOP-004-1 was submitted to the Commission for approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[45] Although the Commission did not address EOP-004-1 R1 directly, in Order No. 693 at paragraph 617 it stated that EOP-004-1:

> . . . serves an important purpose in establishing requirements for reporting and analysis of system disturbances. Accordingly, the Commission approves Reliability Standard EOP-004-1 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission directs the ERO to develop a modification to EOP-004-1 through the Reliability Standards development process that includes any Requirements necessary for users, owners and operators of the Bulk-Power System to provide data that will assist NERC in the investigation of a blackout or disturbance.

The directive to provide data that will assist NERC in the investigation of a blackout or disturbance is not affected by the EOP-004-1 R1, because that is accomplished via other requirements in EOP-004-1 and is also under consideration for enhancement in the development of EOP-004-2.

Technical Justification

The reliability purpose of EOP-004-1 is to ensure that disturbances or unusual occurrences that jeopardize the operation of the BES, or result in system equipment damage or customer interruptions, are studied and understood in order to minimize the likelihood of similar events in the future. The reliability purpose of EOP-004-1 is unaffected by the proposed retirement of R1.

EOP-004-1 R1 is an anomaly in the Reliability Standards, given that it requires the Regional Reliability Organization to develop a reporting procedure. Although the development of such a reporting procedure may be helpful guidance to responsible entities on reporting of disturbances to Regional Entities, in and of itself is an administrative and documentation task that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B3). It is worth noting that EOP-004-1 R1, like CIP-001-2a R4, is administrative in that it only requires the development of procedures, it does not require that they be followed. More importantly, the mandatory processes for reporting preliminary and final disturbance reports are set forth in EOP-004-1 R3 and its sub-requirements which read as follows:

> R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

[45] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

> R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.
>
> R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2- EOP-004.
>
> R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.
>
> R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

There is no reliability gap created by the passive retirement of EOP-004-1 R1, because EOP-004-1 R3 and its sub-requirements require considerable action to report on disturbances.[46] Also, consider that the EOP-004-1 R1 regional procedures may take the lead from NERC, and, therefore, the regional procedures become a reiteration or a hybrid of mandatory (EOP-004-1 R3 and its sub-requirements) and voluntary rules (NERC

[46] While not dispositive, the NERC voluntary event analysis process is also being used to report and analyze events. A link to NERC's event analysis process is http://www.nerc.com/page.php?cid=5|365.

Event Analysis Process).[47] It is an unnecessarily burdensome task to require such reiterations of NERC reporting requirements on a regional level. Also, if there was a need for particular regional procedures such procedures could exist as guidance even without the existence of EOP-004-1 R1. Thus, the value of EOP-004-1 R1 as a Reliability Standard requirement to support reliability is diminutive.

Furthermore, the retirement of EOP-004-1 R1 will increase the efficiency of the ERO compliance program in that the time and resources spent monitoring EOP-004-1 and checking off whether or not a Regional Entity has the specified procedure, and can be utilized to focus attention on an entity's compliance with EOP-004-1 R3 and its sub-requirements, which produce the information related to disturbances.

Criterion A
A requirement that Regional Entities develop a reporting procedure in and of itself is an administrative and documentation task that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C
1. EOP-004-1 R1 has not been part of a FFT filing.

2. EOP-004-1 R1 is part of an on-going Standards Development Project 2009-01 (EOP-004-2) and is being proposed for retirement as unnecessary. At this time, EOP-004-2 has not been approved by stakeholders and the NERC Board of Trustees, and, therefore, it is appropriate to retain EOP-004-1 R1 within the scope of the P81 Project. However, if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 Project and may include EOP-004-1 R1 for informational purposes only.

3. The VRF for EOP-004-1 R1 is Lower.

4. EOP-004-1 R1 is in the third tier of the AML.

5. The retirement of EOP-004-1 R1 does not pose any negative impact to NERC's published and posted reliability principles, as none of the principles are directly implicated.

[47] *See, e.g.*, FRCC Disturbance Reporting Procedure, FRCC – RE – OP – 001-0 Effective Date – February 10, 2012.

6. The retirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of EOP-004-1 R1 promotes a results-based approach because the requirement is an administrative task of developing a procedure with no associated actionable performance of a task that impacts reliability.

Accordingly, for the above reasons, it is appropriate to retire EOP-004-1 R1.

EOP-005-2 R3.1– System Restoration from Blackstart Resources

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

Background/Commission Directives

EOP-005-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[48] EOP-005-2 was submitted for Commission approval on December 31, 2009 in Docket No. RM10-16-000 and was approved on March 17, 2011 in Order No. 749.[49] Although the Commission did not address EOP-005-2 R3 directly in Order No. 749, it stated at paragraph 17 the following:

> EOP-005-2 and EOP-006-2 clarify the responsibilities of the reliability coordinator and transmission operator in the restoration process and restoration planning and address the Commission's directives in Order No. 693 related to the EOP Standards. By enhancing the rigor of the restoration planning process, the Reliability Standards represent an improvement from the current Standards and will improve the reliability of the Bulk-Power System. The Commission is not directing any modifications to the three new Reliability Standards. Nevertheless, as discussed below, commenters raised several issues for consideration, at the time these standards are next revisited, which we believe could improve these new Reliability Standards

There are no outstanding Commission directives that are affected by the proposed retirement of EOP-005-2 R3.1.

[48] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 (2007).
[49] *System Restoration Reliability Standards*, 134 FERC ¶ 61,215, (March 17, 2011) ("Order No. 749"), *order on clarification*, 136 FERC ¶ 61,030 ("Order No. 749-A") (2011).

Technical Justification

The reliability purpose of EOP-005-2 is to ensure that plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure that reliability is maintained during restoration and priority is placed on restoring the Interconnection. This reliability purpose is unaffected by the proposed retirement of R3.1.

A review of EOP-005-2 R3.1 indicates that this requirement is redundant with EOP-005-2 R3 and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1, B5 and B7). The primary reason EOP-005-2 R3.1 is unnecessary is that EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes. EOP-005-2 R3 reads:

> Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule.

Consequently, since R3 requires the Transmission Operator to submit its restoration plan to the Reliability Coordinator whether or not there has been a change, R3.1 only adds a separate, duplicative administrative burden for the entity to also confirm that there were no changes based upon another pre-determined schedule. While R3.1 may have attempted to capture the likelihood that unless there have been significant changes to the entity's BES, there would be no change to the restoration plan, this is an insufficient reason to impose a needlessly burdensome, duplicative administrative requirement relative to the language in R3. EOP-005-2 R3.1 is also clearly needlessly burdensome if one considers that the time and resources of Transmission Operators is better spent reliably operating the BES, rather than submitting paperwork to a Reliability Coordinator on possibly two different pre-determined schedules – one for changes and one for no changes. For these reasons, there is no reliability gap resulting from the retirement of EOP-005-2 R3.1 because Transmission Operators already have an obligation to review and provide its restoration plan annually on a mutually agreed predetermined schedule to its Reliability Coordinator. It could also be argued that a reason for both R3 and R3.1 is for the Reliability Coordinator to organize the Transmission Operator submittals into changes versus no changes. However, with the requirement to annually review restoration plans comes the need to demonstrate and track annual reviews via the revision history index, for example, which quickly shows the Reliability Coordinator when changes have and have not occurred.

The retirement of EOP-005-2 R3.1 would also increase the efficiencies of the ERO compliance program because the ERO would be able to focus its time and resources on R3 which already captures R3.1 and not be concerned with tracking the submission of restoration plans on multiple pre-determined schedules, some with changes and some without changes. Instead, the focus of the ERO compliance program would be on whether the Transmission Operators annually submitted its restoration plan to its

Reliability Coordinator on one pre-determined schedule. Thus, the retirement of EOP-005-2 R3.1 appears to benefit the ERO compliance program.

Criterion A
EOP-005-2 R3.1 is redundant and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)
- Criterion B5 (Periodic Updates)
- Criterion B7 (Redundant)

Criteria C
1. EOP-005-2 R3.1 has not been part of a FFT filing.

2. EOP-005-2 R3.1 is not part of an on-going Standards Development Project.

3. EOP-005-2 R3.1 does not yet have a FERC-approved VRF.

4. EOP-005-2 R3.1 is on the second tier of the AML; however, the duplicative nature of R3 and R3.1 discounts any indication that R3.1 being in the second tier is a reason not to proceed with its retirement.

5. Since EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes, retirement of EOP-005-2 R3.1 does not pose any negative impact to the following of NERC's published and posted reliability principles that appear to apply:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

6. Retirement of EOP-005-2 R3.1 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of EOP-005-2 R3.1 promotes a results-based approach because the requirement is administrative and unnecessary, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire EOP-005-2 R3.1.

FAC-002-1 R2 – Coordination of Plans for New Facilities

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

Background/Commission Directives
FAC-002-0 was submitted to the Commission for approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[50] FAC-002-1 was submitted for Commission approval on September 9, 2010 in Docket No. RD10-15-000 and was approved on January 10, 2011.[51] When approving FAC-002-0 in Order No. 693 at paragraphs 692 and 693, and FAC-002-1 in a subsequent order,[52] the Commission did not directly address R2.

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-002-1 R2.

Technical Justification
Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, without the existence of FAC-002-1 R2, a Regional Entity or NERC has the ability to request and receive "documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems)." This generally would occur during a spot check or compliance audit where entities have the obligation to provide documentation sufficient to demonstrate compliance. In this regard, entities already have the obligation to produce the same information required in R2 to demonstrate compliance to R1 and its sub-requirements, thus making R2 unnecessary. To have a Reliability Standard requirement that is setting forth a data retention requirement and a requirement for the entity to deliver, upon request, that data to NERC

[50] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[51] NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2 RD10-15-000 (January 10, 2011).
[52] *North American Electric Reliability Corporation*, 134 FERC ¶ 61,015 (2011).

or a Regional Entity is unnecessary and also repetitive with the NERC Rules of Procedure. Accordingly, retiring FAC-002-1 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. Thus, FAC-002-1 R2 is not necessary to support reliability. Consequently, a review of R2 indicates that it is an administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). The compilation of three years of data is a burdensome task, particularly when one considers the resources and time spent on stockpiling this information is better spent coordinating the studies, executing an interconnection agreement and ensuring that interconnections are safely and reliably energized, maintained and operated. Also, there are some inherent inefficiencies that result from a small number of requirements, such as CIP-007-3, -4 R7.3 and FAC-002-1 R2 being data, evidence and record retention requirements, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A

A review of FAC-002-1 R2 indicates that it is an administrative and data collection requirement that does little, if anything, to benefit or protect reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. FAC-002-1 R2 has not been part of a FFT filing.

2. FAC-002-1 R2 is subject to a future Project 2010-02 Connecting New Facilities to the Grid (a review of FAC-001 and FAC-002) that is scheduled to begin in the second quarter of 2015. It seems appropriate to retire FAC-002-1 R2 at this time as it may also make the review of FAC-001 and FAC-002 more effective and efficient.

3. FAC-002-1 R2 has a Lower VRF.

4. FAC-002-1 R2 is in the third tier of the AML.

5. The retirement of FAC-002-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since there are no directly applicable reliability principles.

6. The retirement does not negatively impact defense in depth because the compilation of studies for three years has no operational or planning relationship with any other requirement.

7. The retirement of FAC-002-1 R2 promotes a results-based approach since the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-002-1 R2.

FAC-008-1 R2; FAC-008-1 R3;[53] - Facility Ratings Methodology

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

Background/Commission Directives
FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[54]

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-1 R2 and R3.

[53] Unlike the other requirements presented for informational purposes only, FAC-008-1 R2 and FAC-008-1 R3 have been maintained within the scope of P81 given that they are essentially identical to FAC-008-3 R4; FAC-008-3 R5 which are due be effective on January 1, 2013. Inclusion would also appear to be consistent with increasing ERO compliance program efficiencies, given that retirement would exempt these requirements from being included in spot checks or compliance audits that are backward looking via FAC-008-1 R2 and R3.

[54] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Technical Justification

FAC-008-1 R2 and R3 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-1 R2 and R3 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-1 regarding their facility rating methodologies whether or not the exchange envisioned by FAC-008-1 R2 and R3 occurs. Furthermore, neither FAC-008-1 R2 and R3 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-1 R2 and R3 are designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its generator step up ("GSU") transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, operating conditions, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of System Operating Limits ("SOLs"), Interconnection Reliability Operating Limits ("IROLs"), calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments).[55] Accordingly, the requirements in FAC-008-1 R2 and FAC-008-1 R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange of comments and compliance with the substantive

[55] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-02 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element.

requirements of FAC-008-1. Instead of spending time and resources on FAC-008-1 R2 and R3, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-1.

Criterion A

The requirements in FAC-008-1 R2 and R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-008-1 R2 and R3 have not been part of a FFT filing.

2. FAC-008-1 R2 and R3 are not subject to an on-going Standards Development Project.

3. FAC-008-1 R2 and R3 have a Lower VRF.

4. FAC-008-1 R2 and R3 are in the third tier of the AML.

5. The retirement of FAC-008-1 R2 and R3 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-008-1 that promotes these posted reliability principles, and not receiving comments on the facility

ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-1 R2 and R3, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These requirements may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-1 R2 and R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-1 R2 and R3.

FAC-008-3 R4; FAC-008-3 R5 – Facility Ratings

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.

Background/Commission Directives

FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[56] "On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No. 693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order

[56] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[57] FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[58]

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-3 R4 and R5.

Technical Justification

FAC-008-3 R4 and R5 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-3 R4 and R5 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-3 regarding their facility rating methodologies whether or not the exchange envisioned by FAC-008-3 R4 and R5 occurs. Further, neither FAC-008-3 R4 nor R5 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-3 R4 and R5 are designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its GSU transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, historical performance, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of SOLs, IROLs, calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments).[59] Accordingly, the

[57] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[58] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).
[59] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-2 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may

requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-008-3. Instead of spending time and resources on FAC-008-3 R4 and R5, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-3. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-3.

Criterion A

The requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-008-3 R4 and R5 have not been part of a FFT filing.

2. FAC-008-3 R4 and R5 are not subject to an on-going Standards Development Project.

3. FAC-008-3 R4 and R5 have a Lower VRF.

4. FAC-008-3 R4 and R5 are in the third tier of the AML.

5. The retirement of FAC-008-3 R4 and R5 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under

---

also use facility ratings as a key element. Also, FAC-008-3 R7 and R8 require the transmission of facility ratings to reliability entities.

normal and abnormal conditions as defined in the NERC Standards.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-008-3 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-3 R4 and R5, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-3 R4 and R5 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-3 R4 and R5.

****FAC-010-2.1 R5 – System Operating Limits Methodology for the Planning Horizon**

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives

FAC-010-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[60] FAC-010-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[61] FAC-010-2.1 was filed for Commission approval on November 20, 2009 in Docket No. RD10-9-000

[60] *Facilities Design, Connections and Maintenance Reliability Standards,* 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).

[61] *Version Two Facilities Design, Connections and Maintenance Reliability Standards,* 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).

and was approved on April 19, 2010.[62] In Order No. 722,[63] the Commission approved FAC-010-2.1 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

Technical Justification

The reliability purpose of FAC-010-2.1, to ensure that System Operating Limits used in the reliable planning of the BES are determined based on an established methodology, is unaffected by the proposed retirement of R5. FAC-010-2.1 R5 requires that when a Planning Authority receives comments on its SOL methodology, it must respond and indicate whether it has changed its methodology. The retirement of FAC-010-2.1 R5 does not create a reliability gap, because the Planning Authority must comply with the substantive requirements of FAC-010-2.1 whether or not the exchange envisioned by FAC-010-2.1 R5 occurs. FAC-010-2.1 R5 may support an avenue to advance commercial interests.

For example, if a Transmission Operator or Transmission Planner is also a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Planning Authority's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of its development of a facility ratings methodology under FAC-008-1, -3 than the Planning Authority's methodology. FAC-010-2.1 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Planning Authority's SOL methodology. Accordingly, FAC-010-2.1 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-010-2.1. Instead of spending time and resources on FAC-010-2.1, a Planning Authority's time and resources would be better spent complying with the substantive requirements of FAC-010-2.1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Planning Authority's adherence to substantive requirements of FAC-010-2.1.

Criterion A

The requirement in FAC-010-2.1 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

[62] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Transmission Operations Reliability Standards, Docket No. RD10-9-000 (April 19, 2010).

[63] *Version Two Facilities Design, Connections and Maintenance Reliability Standards* 125 FERC ¶ 61,040 (2009).

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-010-2.1 R5 has not been part of a FFT filing.

2. FAC-010-2.1 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011. Thus, it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-010-2.1 R5 has a Lower VRF.

4. FAC-010-2.1 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-010-2.1 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-010-2.1 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-010-2.1 R5.

****FAC-011-2 R5– System Operating Limits Methodology for the Operations Horizon**

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives

FAC-011-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[64] FAC-011-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[65] In Order No. 722, the Commission approved FAC-011-2 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

Technical Justification

FAC-011-2 R5 requires that when a Reliability Coordinator receives comments on its SOL methodology that it must respond and indicate whether it has changed its methodology. The retirement of FAC-011-2 R5 does not create a reliability gap, because the Reliability Coordinator must comply with the substantive requirements of FAC-011-2 R5 whether or not the exchange envisioned by FAC-011-2 R5 occurs. FAC-011-2 R5 may support an avenue to advance commercial interests.

For example, similar to FAC-010-2.1 R5, if a Transmission Operator or Transmission Planner also is a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Reliability Coordinator's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of the development of its facility ratings methodology under FAC-008-1, -3 than the Reliability Coordinator's methodology. FAC-011-2 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Reliability Coordinator's SOL methodology. Accordingly, FAC-011-2 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In

[64] *Facilities Design, Connections and Maintenance Reliability Standards,* 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).

[65] *Version Two Facilities Design, Connections and Maintenance Reliability Standards,* 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).

this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-011-2. Instead of spending time and resources on FAC-011-2 R5 a Reliability Coordinator's time and resources would be better spent complying with the substantive requirements of FAC-011-2 R5. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-011-2 R5.

Criterion A
The requirement in FAC-011-2 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-011-2 R5 has not been part of a FFT filing.

2. FAC-011-2 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011which is not currently scheduled and thus it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-011-2 R5 has a Lower VRF.

4. FAC-011-2 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-011-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-011-2 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-011-2 R5.

FAC-013-2 R3 – Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.

Background/Commission Directives

FAC-013-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[66] FAC-013-2 was submitted for Commission approval on January 28, 2011 in Docket No. RD11-3-000 and was approved on November 17, 2011.[67]

In Order No. 729, the Commission denied NERC's request to withdraw FAC-012-1 and retire FAC-013-1, and directed as follows at paragraph 291:

> 291. The Commission hereby adopts its NOPR proposal to deny NERC's request to withdraw FAC-012-1 and retire FAC-013-1. Instead, pursuant to section 215(d)(5) of the FPA and section 39.5(f) of our regulations, the Commission directs the ERO to develop modifications to FAC-012-1 and FAC-013-1 to comply with the relevant directives of Order No. 693 and, as otherwise necessary, to make the requirements of those Reliability Standards consistent with those of the MOD Reliability Standards approved herein as well as this Final Rule. These

[66] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[67] *Order Approving Reliability Standard*, 137 FERC ¶ 61,131 (2011).

> modifications should also remove redundant provisions for the calculation of transfer capability addressed elsewhere in the MOD Reliability Standards. In making these revisions, the ERO should consider the development of a methodology for calculation of inter-regional and intra-regional transfer capabilities. The Commission accepts the ERO's request for additional time to prepare the modifications and so directs the ERO to submit the modifications to FAC-012-1 and FAC-013-1 no later than 60 days before the MOD Reliability Standards become effective.

Although the Commission did not directly address the merits of FAC-013-2 R3 when approving FAC-013-2,[68] similar to FAC-008-3, the developer of the Transfer Capability methodology and data must follow specific technical requirements and provide the data to reliability entities for use in their models. There are no outstanding Commission directives with respect to this R3.

Technical Justification

A review of FAC-013-2 R3 indicates that it is a needlessly burdensome administrative task that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B4). Specifically, FAC-013-2 R1 and its sub-requirements set forth the information that each Planning Authority must include when developing its Transfer Capability methodology. FAC-013-2 R3 sets forth a requirement that if an entity comments on this methodology, the Planning Authority must respond and indicate whether or not it will make a change to its Transfer Capability methodology. Thus, while R1 sets forth substantive requirements, R3 sets forth more of an administrative task of the Planning Authority responding to comments on its methodology.

The following NERC glossary definition of Transfer Capability states:

> The measure of the ability of interconnected electric systems to move or transfer power *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is *not g*enerally equal to the transfer capability from "Area B" to "Area A."

In the context of a Planning Authority engaging in an exchange with an entity over the Transfer Capability there is a possibility of a scenario that a group of generators[69] try to get the Planning Authority to revise its Transfer Capability methodology to advance commercial interests via changes to the methodology that would increase or decrease transfer capability from Area A to Area B. (Criterion B6). Such issues should be raised

[68] *Id.* (approval of FAC-013-2).

[69] Generators that receive the Transfer Capability methodology via an association with one of the entities in the R2 sub-requirements.

in the context of receipt of transmission services, not the Reliability Standards. Moreover, even without the possible commercial motivation of certain entities to get the Planning Authority to revise its Transfer Capability methodology, implementing an exchange between entities and the Planning Authority seems much better suited via regional planning committees, than mandatory Reliability Standards.

In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-013-2. Instead of spending time and resources on FAC-013-2 R3, time and resources would be better spent complying with the substantive requirements of FAC-013-2. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-013-2.

Criterion A
The requirement in FAC-013-2 R3 to respond to comments on the Transfer Capability methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-013-2 R3 has not been part of a FFT filing.

2. FAC-013-2 R3 is not subject to an on-going Standards Development Project.

3. FAC-013-2 R3 has a Lower VRF.

4. FAC-013-2 R3 is not on the AML.

5. The retirement of FAC-013-2 R3 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-013-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of FAC-013-2 R3 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-013-2 R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-013-2 R3.

INT-007-1 R1.2 – Interchange Confirmation

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

Background/Commission Directives
INT-007-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[70] The Commission did not directly address INT-007-1 R1.2 when it approved the Reliability Standard in Order No. 693 at paragraph 867.

There are no outstanding Commission directives with respect to R1.2.

Technical Justification
The reliability purpose of INT-007-1 is to ensure that each Arranged Interchange is checked for reliability before it is implemented. The reliability purpose of INT-007-1 is unaffected by the proposed retirement of R1.2.

INT-007-1 R1.2 is a needlessly burdensome administrative task that does not support reliability because it is now outdated. (Criterion B1). At one time the identification number came from the NERC TSIN system, by now it is handled via NAESB Electric

[70] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Industry Registry.[71] Also, under the E-Tag protocols, no entity may engage in an Interchange transaction without first registering with the E-Tag system and receiving an identification number. Further, the entity desiring the transaction enters this identification number in the E-Tag system to pre-qualify and engage in an Arranged Interchange. Accordingly, the task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A). The ERO compliance program would benefit and be more efficient if it was not monitoring an outdated requirement.

Criterion A
The task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. INT-007-1 R1.2 has not been part of a FFT filing.

2. INT-007-1 R1.2 is part of a pending Standards Development Project – Project 2008-12 Coordinate Interchange Standards, which is estimated to start in the second quarter of 2013. Given this timeline, it is appropriate to move forward with the retirement of INT-007-1 R1.2. Such a retirement may also help to streamline Project 2008-12 once it is active and progressing.

3. INT-007-1 R1.2 has a Lower VRF.

4. INT-007-1 R1.2 is not on the AML.

5. The retirement of INT-007-1 R1.2 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

    Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

    Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

[71] *See, North American Energy Standards Board Webregistry Technical Guide v1.4* (Proprietary) (July 2012). The new NAESB system has updated and implemented more automation to the process.

It is the adherence to the substantive requirements of INT-007-1 that promotes these posted reliability principles, not R1.2.

6. The retirement of INT-007-1 R1.2 does not impact any defense in depth strategies because the task is no longer necessary.

7. The retirement of INT-007-1 R1.2 promotes a results-based approach because the requirement does not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire INT-007-1 R1.2.

IRO-016-1 R2 – Coordination of Real-time Activities Between Reliability Coordinators

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

Background/Commission Directives
IRO-016-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693. The Commission did not directly address R2 when approving IRO-016-1 in Order No. 693 at paragraphs 1004 and 1005. There are no outstanding Commission directives with respect to R2.

Technical Justification
The reliability purpose of IRO-016-1 is to ensure that each Reliability Coordinator's operations are coordinated such that they will not have an adverse reliability impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations. To implement the purpose, IRO-016-1 R1 and its sub-requirements state:

> **R1.** The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
>
> **R1.1.** If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.

> **R1.2.** If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
>
> **R1.2.1.** If time permits, this re-evaluation shall be done before taking corrective actions.
>
> **R1.2.2.** If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

These requirements are specific actions and decision points among Reliability Coordinators that promote the reliable operation of the BES. In contrast, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Therefore, the reliability purpose of IRO-016-1 is unaffected by the proposed retirement of R2.

Furthermore, outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, the retirement of IRO-016-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to demonstrate compliance with IRO-016-1 R1 and its sub-requirements. Accordingly, retiring IRO-016-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. Thus, IRO-016-1 R1 does not support reliability. Consequently, R2 is an administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as IRO-016-1 R2 being a data, evidence and record retention requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A
A review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. IRO-016-1 R2 has not been part of a FFT filing

2. IRO-016-1 R2 is not subject to an on-going Standards Development project.

3. IRO-016-1 R2 has a Lower VRF.

4. IRO-016-1 R2 is not on the AML.

5. The retirement of IRO-016-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since none of the principles appear to apply to a data retention requirement.

6. IRO-016-1 R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of IRO-016-1 R2 promotes a results-based approach because the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire IRO-016-1 R2.

NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4 – Nuclear Plant Interface Coordination

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement.

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3. A requirement to review the agreement(s) at least every three years.

R9.1.4. A dispute resolution mechanism.

Background/Commission Directives

NUC-001-1 was submitted for Commission approval on November 19, 2007 in Docket No. RM08-3-000 and was approved on October 16, 2008.[72] NUC-001-2 was submitted

[72] *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008) ("Order No. 716"), *order on reh'g*, Order No. 716-A, 126 FERC ¶ 61,122 (2009).

for Commission approval on August 14, 2009 in Docket No. RD09-10-000 and was approved on January 21, 2010.[73]

Although in Order No. 716 the merits of R9.1 and its sub-requirements were not directly addressed, the Commission did state the following in the context of the VRFs for all of R9:[74]

> Consistent with the NOPR, the Commission directs the ERO to revise the violation risk factor assignment for Requirement R9 from lower to medium. The Commission disagrees with commenters that a lower violation risk factor is appropriate because Requirement R9 is an administrative requirement to include the specified provisions. While the Commission recognized in the NOPR that many of the requirements of the proposed Reliability Standard are administrative in nature, these same requirements provide for the development of procedures to ensure the safe and reliable operation of the grid, and responses to potential emergency conditions.

There are no outstanding Commission directives with respect to these requirements.

Technical Justification

The reliability purpose of NUC-001-2 is to ensure the coordination between Nuclear Plant Generator Operators and Transmission Entities for nuclear plant safe operation and shutdown. The reliability purpose of NUC-001-2 is unaffected by the proposed retirement of requirements 9.1, 9.1.1, 9.1.2, 9.1.3 and 9.1.4. Requirement 9.1 and its sub-requirements specify certain administrative elements that must be included in the agreement (required by R2) between the Nuclear Plant Generator Operator and the applicable Transmission Entities. These are a mix of technical, communication, training and administrative requirements. Of those that may be classified as administrative, R9.1 and its sub-requirements clearly stand out as unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A and B1). R9.1 and its sub-requirements are a check list of certain non-technical boilerplate provisions generally included in modern agreements. These provisions do not directly relate to protecting BES reliability. Further, requiring via a mandatory Reliability Standard the inclusion of boilerplate provisions is an unnecessarily burdensome relative to the other significant requirements in NUC-001-2 that pertain to performance based reliability coordination and protocols between Transmission Entities and Nuclear Plant Generator Operators. Therefore, the retirement of NUC-001-2 R9.1 and all its sub-requirements creates no reliability gap and are the type of provisions that would likely be in a modern agreement anyway.

---

[73] *Order Approving Reliability Standard*, 130 FERC ¶ 61,051 (2010).

[74] NUC-001-1 was approved in Order No. 716, while NUC-001-2 was approved without discussion of R9.1 and its sub-requirements in a subsequent order. *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008); 130 FERC ¶ 61,051 (2010).

For these same reasons, the ERO compliance program efficiency will increase with the retirement of NUC-001-2 R9.1 and its sub-requirements because compliance monitoring time and resources will not be spent conducting a checklist of whether an agreement includes boilerplate provisions, and instead, the time and resources may be spent reviewing adherence with the technical, substantive coordination and protocol provisions of NUC-001-2.

Criterion A
R9.1 and its sub-requirements are unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)

Criteria C
1. NUC-001-2 R9.1 and its sub-requirements have not been part of a FFT filing.

2. NUC-001-2 R9.1 and its sub-requirements are not part of an on-going Standards Development Project, but NUC-001-2 is part of Project 2012-13, which is a placeholder for a five year review. Given the as yet undetermined start date for Project 2012-13, it is appropriate to move forward with the retirement of NUC-001-2 R9.1 and its sub-requirements.

3. Individual VRFs are not assigned to the sub-requirements of NUC-001-2 R9.

4. NUC-001-2 R9.1 and its sub-requirements are in the third tier of the AML.

5. The retirement of NUC-001-2 R9.1 and its sub-requirements do not pose any negative impact to NERC's published and posted reliability principles, since none of them seem to apply to the inclusion of boilerplate contractual provisions.

6. There is no impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of NUC-001-2 R9.1 and its sub-requirements promote a results-based approach by eliminating administrative check-list requirements.

Accordingly, for the above reasons, it is appropriate to retire NUC-001-2 R9.1 and its sub-requirements.

PRC-010-0 R2 – Assessment of the Design and Effectiveness of UVLS Program;

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide

> documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

Background/Commission Directives

PRC-010-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[75] Although not specifically addressing PRC-010-0 R2, in Order No. 693 at paragraph 1506 and 1507 the Commission stated that:

> With regard to ISO-NE's disagreement on integration of various system protections "because such integration cannot be technologically accomplished", we note that the evidence collected in the Blackout Report indicates that "the relay protection settings for the transmission lines, generators and underfrequency load shedding in the northeast may not be entirely appropriate and are certainly not coordinated and integrated to reduce the likelihood and consequence of a cascade – nor were they intended to do so." In addition, the Blackout Report stated that one of the common causes of major outages in North America is a lack of coordination on system protection. The Commission agrees with the protection experts who participated in the investigation, formulated Blackout Recommendation No. 21 and recommended that UVLS programs have an integrated approach.
>
> Regarding FirstEnergy's question of whether universal coordination among UVLS programs that address local system problems makes sense, we believe that PRC-010-0's objective in requiring an integrated and coordinated approach is to address the possible adverse interactions of these protection systems among themselves and to determine whether they could aggravate or accelerate cascading events. We do not believe this Reliability Standard is aimed at universal coordination among UVLS programs that address local system problems. (Footnote omitted).

The retirement of PRC-010-0 R2 does not affect a Commission directive.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its current UVLS program assessment for purposes of monitoring compliance. Thus, the retirement of PRC-010-0 R2 does not affect the ability of NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-010-0 R1 and its sub-requirements.

[75] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Furthermore, PRC-010-0 R1 requires that the entity document an assessment of the effectiveness of its UVLS program:

> The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program.

Accordingly, retiring PRC-010-0 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. A review of R2 indicates that it is a needlessly burdensome administrative and data collection/retention requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as PRC-010-0 R2 being a data production requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401.

Criterion A
R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C
1. PRC-010-0 R2 has not been part of a FFT filing.

2. PRC-010-0 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-010-0 R2 in the P81 Project.

3. This requirement has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-010-0 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-010-0 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-010-0 R2.

PRC-022-1 R2 – Under-Voltage Load Shedding Program Performance

> **R2.** Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

Background/Commission Directives
PRC-022-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[76] In Order No. 693 at paragraph 1565 the Commission approved PRC-022-1 without a discussion of R2. There are no outstanding Commission directives with respect to R2.

Technical Justification
Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its analysis of UVLS program performance for purposes of monitoring compliance. Thus, the retirement of PRC-022-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-022-1 R1 and its sub-requirements. Furthermore, PRC-022-1 R1 already requires that the entity document UVLS performance:

> Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations.

Accordingly, retiring PRC-022-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. In this context, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of

[76] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

the BES. (Criteria A, B1 and B2). Also, similar to the retention of records requirements in CIP-007-3, -4 R7.3, FAC-002-1 R2 and PRC-010-0 R2, the ERO compliance program efficiency will increase since it will no longer need to track a static requirement of whether a UVLS program assessment was submitted within 30 days of a request by NERC or the Regional Entity, and instead, compliance monitoring may focus on the more substantive requirements of PRC-022-1.

Criterion A
R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C
1. PRC-022-1 R2 has not been part of a FFT filing.

2. PRC-022-1 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-022-1 R2 in the P81 Project.

3. PRC-022-1 R2 has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-022-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-022-1 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-022-1 R2.

****VAR-001-2 R5 – Voltage and Reactive Control**

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

Background/Commission Directives

VAR-001-1 was submitted for Commission approval on April 4, 2006, in Docket No. RM06-16-000. When approving VAR-001-1, in Order No. 693 at paragraph 1858,[77] the Commission recognized:

> . . . that all transmission customers of public utilities are required to purchase Ancillary Service No. 2 under the OATT or self-supply, but the OATT does not require them to provide information to transmission operators needed to accurately study reactive power needs. The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities.

On September 9, 2010, NERC submitted VAR-001-2, which included revisions to Requirement R5 to satisfy Commission directives in Order No. 693, including the directive in paragraph 1858. This directive was addressed by adding "Load Serving Entities" to the standard as applicable entities and making them subject to the same requirements as Purchasing Selling Entities. These modifications to VAR-001-2 were accepted by the Commission on January 10, 2011.[78]

Technical Justification

VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* open access transmission tariff ("OATT"). (Criteria A and B7). To elaborate, VAR-001-2 R5 provides for the PSE and LSE (transmission customers) to arrange for or self provide reactive resources the same as required under Schedule 2 of the OATT. Specifically, as a general matter Schedule 2 of the OATT states:

> **Schedule 2 Reactive Supply and Voltage Control from Generation or Other**
>
> In order to maintain transmission voltages on the Transmission Provider's transmission facilities within acceptable limits, generation facilities and non-generation resources capable of providing this service that are under the control of the control area operator) are operated to produce (or absorb) reactive power. Thus, Reactive Supply and Voltage Control from

[77] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[78] *North American Electric Reliability Corp.*, 134 FERC ¶ 61,015 (2011).

> Generation or Other Sources Service must be provided for each transaction on the Transmission Provider's transmission facilities. The amount of Reactive Supply and Voltage Control from Generation or Other Sources Service that must be supplied with respect to the Transmission Customer's transaction will be determined based on the reactive power support necessary to maintain transmission voltages within limits that are generally accepted in the region and consistently adhered to by the Transmission Provider.
>
> Reactive Supply and Voltage Control from Generation or Other Sources Service is to be provided directly by the Transmission Provider (if the Transmission Provider is the Control Area operator) or indirectly by the Transmission Provider making arrangements with the Control Area operator that performs this service for the Transmission Provider's Transmission System. The Transmission Customer must purchase this service from the Transmission Provider or the Control Area operator. A Transmission Customer may satisfy all or part of its obligation through self provision or purchases provided that the self-provided or purchased reactive power reduces the Transmission Provider's reactive power requirements and is from generating facilities under the control of the Transmission Provider or Control Area operator. The Transmission Customer's Service Agreement shall specify any such reactive supply arrangements. To the extent the Control Area operator performs this service for the Transmission Provider, charges to the Transmission Customer are to reflect only a pass-through of the costs charged to the Transmission Provider by the Control Area operator. The Transmission Provider's rates for Reactive Supply and Voltage Control from Generation Sources Services shall be set out in Appendix A to this Schedule.

Given the importance of the procurement or self providing of reactive power, even in a market setting a form of Schedule 2 is found in the tariffs of MISO and PJM, for example. While NERC complied with the Commission's directive to add LSEs to VAR-001-2 R5, a review of this requirement in light of Schedule 2 indicates that the reliability objective of ensuring that PSEs as well as LSEs either acquire or self provide reactive power resources associated with its transmission service requests is accomplished via Schedule 2, and, therefore, there is no need to reiterate it in VAR-001-2 R5. The repetitive nature of VAR-001-2 R5 is also apparent in the context of how a PSE or LSE generally demonstrates compliance – via screenshots from Open Access Same-Time Information System ("OASIS") reservations that show the mandatory acquiring or self providing of reactive power resources per Schedule 2.

The reliability objective of VAR-001-2 is also accomplished in VAR-001-2 R2 (that is not proposed for retirement) which reads:

> Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, [sic] and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

The Transmission Operator's adherence to R2 is a double check for the obligations under Schedule 2 to ensure there are sufficient reactive power resources to protect the voltage levels under normal and Contingency conditions.

In addition, in the Electric Reliability Council of Texas (ERCOT) region, where there is no FERC approved OATT, reactive power is handled via Section 3.15 of the ERCOT Nodal Protocols that describes how ERCOT establishes a Voltage Profile for the grid, and then in detail explains the responsibilities of the Generators, Distribution Providers and Texas Transmission Service Providers (not to be confused with a NERC TSP), to meet the Voltage Profile and ensure that those entities have sufficient reactive support to do so. There is further Operating Guide detail on the responsibilities for entities to deploy reactive resources approximately, within performance criteria in the Operating Guide Section 3. Thus, as in non-ERCOT regions, ERCOT has protocols that are duplicative of VAR-001-2 R5.

Given the redundant nature of VAR-001-2 R5 it would also assist the ERO compliance program to retire it, so that time and resources can be reallocated to focus on adherence to other Reliability Standard requirements.

Criterion A
VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* OATT.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. VAR-001-2 R5 has not been part of a FFT filing.

2. VAR-001-2 R5 is subject to Standards Development Project 2008-01 Voltage and Reactive Planning Control. Given that Project 2008-01 is not currently active and is only estimated to be completed until the second quarter of 2014 and the purpose of this project does not necessarily include a review of R5, it is appropriate to include VAR-001-2 R5 in the P81 Project. Also, retiring this requirement via P81 Project may facilitate the efficiency of Project 2008-01.

3. This requirement has a High VRF. However, the reliability objective of VAR-001-2 R5 will be accomplished via Schedule 2 of the OATT, ERCOT protocols

and R2 of VAR-001-2. Thus, the High VRF is not dispositive, and VAR-001-2 R5 remains appropriate for retirement.

4. VAR-001-2 R5 is in the third tier of the AML.

5. Because VAR-001-2 R5 is redundant with the *pro forma* OATT and ERCOT protocols, (as well as the reliability objective of VAR-001-2 R5 is accomplished via Schedule 2 of the OATT, ERCOT protocols and R2 of VAR-001-2), the retirement of VAR-001-2 R5 does not pose any negative impact to the following NERC published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of VAR-001-2 R5 is neutral regarding whether it promotes a results-based approach because the requirement is results-based, but already covered in the *pro forma* OATT, Schedule 2 and ERCOT protocols.

Accordingly, for the above reasons, it is appropriate to retire VAR-001-2 R5.

V. The Initial Phase Reliability Standards Provided for Informational Purposes

The following requirements are already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the NERC Board of Trustees in November), and, thus, are presented here for informational purposes only. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the NERC Board of Trustees for approval or filed with the Commission or Canadian governmental authorities as part of the P81 Project.

COM-001-1.1 R6- Telecommunications

Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."

Background
COM-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[79] COM-001-1.1 was submitted for Commission approval on February 6, 2009 in Docket No. RD09-2-000 as errata and was approved by unpublished letter order on May 13, 2009.[80]

As part of COM-001-2, on September 17, 2012, stakeholders approved the retirement of COM-001-1.1 R6 in Project 2006-06 (Reliability Coordination). This project is due to be presented to the NERC Board of Trustees in November. Thus, COM-001-1 R6 is presented here for informational purposes only.

EOP-009-0 R2 – Documentation of Blackstart Generating Unit Test Results

R2. The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

Background
EOP-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[81] In Order No. 749, the Commission approved the retirement of EOP-009-0 as of July 1, 2013, based on the approval of EOP-005-2, which did not carry forward R2 of EOP-009-0. Thus, EOP-009-0 R2 is presented here for informational purposes only.

FAC-008-1 R1.3.5 – Facility Ratings Methodology

R1.3.5. Other assumptions.

Background
FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[82]

"On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No. 693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order

[79] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[80] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Reliability Coordination and Transmission Operations Reliability Standards, Docket No. RD09-2-000 (May 13, 2009).
[81] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[82] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[83]

FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[84]

FAC-008-3 (which combined FAC-008 and FAC-009) has been approved by the Commission without the "other assumptions" language.[85] Since FAC-008-3 will become effective on January 1, 2013, FAC-008-1 R1.3.5 is presented here for informational purposes only.

PRC-008-0 R1; PRC-008-0 R2 – Underfrequency Load Shedding Equipment Maintenance Programs

R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.

R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).

Background
PRC-008-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[86]

Under Standards Development Project 2007-17 Protection System Maintenance, which recently passed on August 27, 2012, PRC-008-0 is scheduled to be retired, subsumed and replaced with PRC-005-2. PRC-005-2 will likely be presented to the NERC Board of Trustees in November for approval, and, thus, PRC-008-0 is only presented here for informational purposes.

PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2 – UFLS Performance Following an Underfrequency Event

[83] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[84] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).
[85] *Id.*

[86] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UFLS set points and tripping times.

R1.3. A simulation of the event.

R1.4. A summary of the findings.

R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.

Background

PRC-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[87] In Order No. 763 at paragraph 103[88] the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Thus, PRC-009-0 is presented here for informational purposes only.

TOP-001-1a R3 – Reliability Responsibilities and Authorities

R3. Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or

[87] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[88] *Automatic Underfrequency Load Shedding and Load Shedding Plans Re-liability Standards*, 139 FERC ¶ 61,098 (2012).

> Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.

Background

TOP-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved by the Commission on March 16, 2007 in Order No. 693.[89] TOP-001-1a was submitted for approval on July 16, 2010 in Docket No. RM10-29-000 and was approved on September 15, 2011 in Order No. 753.[90]

IRO-001-1a R8 reads:

> Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.

Although there is redundancy between TOP-001-1a R3 and IRO-001-1a R8 as related to Reliability Coordinators, this redundancy was addressed in Standards Development Project 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces TOP-001-1a R3 and reads:

> Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued and identified as such by its Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.

TOP-001-2 has been approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-001-1a R3 is presented for informational purposes only.

TOP-005-2a R1 – Operational Reliability Information

[89] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[90] *Electric Reliability Organization Interpretation of Transmission Operations Reliability Standard*, 136 FERC ¶ 61,176, (September 15, 2011) (Order No. 753).

R1. As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."

Background

Without directly addressing R1 of TOP-005-1 or TOP-005-2a the Commission approved both versions of TOP-005. [91] A review of the Standards Development Project 2007-03 Real-time Transmission Operations indicates it proposes R1 of TOP-005-1 to be retired. The reasoning provided by the SDT was the following:

> Confidentiality is not a reliability issue, but a market or business issue. Since this is not a reliability issue, it does not belong in the Reliability Standards and can be deleted.[92]

As stated above, in the context of Project 2007-03, TOP-001-1a was approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-005-2a R1 is presented for informational purposes only.

[91] Order No. 693 at paragraphs 1648 through 1652 (approval of TOP-005-1); *Mandatory Reliability Standards for Interconnection Reliability Operating Limits,* 134 F.E.R.C. ¶ 61,213 (2011) (approval of TOP-005-2a).

[92] Mapping Document Project 2007-03 Real-time Operations at page 31 (April 27 2012).

Appendix A

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
BAL-005-0.2b	**R2**	√							√			H		No	No	Yes
CIP-001-2a	**R4**	√	√	√	√					√	√	M	2	No	No	Yes
CIP-003-3, -4	**R1.2**	√	√							√	√	L	2	No	No	Yes
CIP-003-3, -4	**R3, R3.1 R3.2 R3.3**	√	√		√					√	√	L	3	No	No	Yes
CIP-003-3, -4	**R4.2**	√	√		√				√	√	√	L	3	No	No	Yes
CIP-005-3a, -4a	**R2.6**	√	√		√					√	√	L	1	No	No	Yes
CIP-007-3, -4	**R7.3**	√	√	√							√	L	1	No	No	Yes
EOP-004-1	**R1**	√	√		√						√	L	3	No	No	Yes
EOP-005-2	**R3.1**	√	√				√		√			N/A	2	No	No	Yes
FAC-002-1	**R2**	√	√	√								L	3	No	No	Yes
FAC-008-1	**R2, R3**	√	√			√		√				L	3	No	No	Yes
FAC-008-3	**R4 R5**	√	√			√		√				L	3	No	No	Yes

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
FAC-010-2.1	**R5****	√	√			√		√				L		No	No	Yes
FAC-011-2	**R5****	√	√			√		√				L		No	No	Yes
FAC-013-2	**R3**	√	√			√		√				L		No	No	Yes
INT-007-1	**R1.2**	√	√									L		No	No	Yes
IRO-016-1	**R2**	√	√	√								L		No	No	Yes
NUC-001-2	**R9.1** **R9.1.1** **R9.1.2** **R9.1.3** **R9.1.4**	√	√									N/A	3	No	No	Yes
PRC-010-0	**R2**	√	√	√								L		No	No	Yes
PRC-022-1	**R2**	√	√	√								L		No	No	Yes
VAR-001-2	**R5****	√							√			H	3	No	No	Yes

Complete Violation Severity Levels Matrix

Encompassing All Commission-Approved Reliability Standards

September 21, 2012

Change History Table is located at the end of the document

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-001-0.1a	R1.	Each Balancing Authority shall operate such that, on a rolling 12-month basis, the average of the clock-minute averages of the Balancing Authority's Area Control Error (ACE) divided by 10B (B is the clock-minute average of the Balancing Authority Area's Frequency Bias) times the corresponding clock-minute averages of the Interconnection's Frequency Error is less than a specific limit. This limit is a constant derived from a targeted frequency bound (separately calculated for each Interconnection) that is reviewed and set as necessary by the NERC Operating Committee. ***See Standard for Formula.***	The Balancing Authority Area's value of CPS1 is less than 100% but greater than or equal to 95%.	The Balancing Authority Area's value of CPS1 is less than 95% but greater than or equal to 90%.	The Balancing Authority Area's value of CPS1 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS1 is less than 85%.
BAL-001-0.1a	R2.	Each Balancing Authority shall operate such that its average ACE for at least 90% of clock-ten-minute periods (6 non-overlapping periods per hour) during a calendar month is within a specific limit, referred to as L_{10}. ***See Standard for Formula.***	The Balancing Authority Area's value of CPS2 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS2 is less than 85% but greater than or equal to 80%.	The Balancing Authority Area's value of CPS2 is less than 80% but greater than or equal to 75%.	The Balancing Authority Area's value of CPS2 is less than 75%.
BAL-001-0.1a	R3.	Each Balancing Authority providing Overlap Regulation Service shall evaluate Requirement R1 (i.e., Control Performance Standard 1 or CPS1) and Requirement R2 (i.e., Control Performance Standard 2 or CPS2) using the characteristics of the combined ACE and combined Frequency Bias Settings.	N/A	N/A	N/A	The Balancing Authority providing Overlap Regulation Service failed to use a combined ACE and frequency bias.
BAL-001-0.1a	R4.	Any Balancing Authority receiving Overlap Regulation Service shall not	N/A	N/A	N/A	The Balancing Authority receiving

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		have its control performance evaluated (i.e. from a control performance perspective, the Balancing Authority has shifted all control requirements to the Balancing Authority providing Overlap Regulation Service).				Overlap Regulation Service failed to ensure that control performance was being evaluated in a manner consistent with the calculation methodology as described in BAL-001-01 R3.
BAL-002-1	R1.	Each Balancing Authority shall have access to and/or operate Contingency Reserve to respond to Disturbances. Contingency Reserve may be supplied from generation, controllable load resources, or coordinated adjustments to Interchange Schedules.	N/A	N/A	N/A	The Balancing Authority does not have access to and/or operate Contingency Reserve to respond to Disturbances.
BAL-002-1	R1.1.	A Balancing Authority may elect to fulfill its Contingency Reserve obligations by participating as a member of a Reserve Sharing Group. In such cases, the Reserve Sharing Group shall have the same responsibilities and obligations as each Balancing Authority with respect to monitoring and meeting the requirements of Standard BAL-002.	N/A	N/A	N/A	The Balancing Authority has elected to fulfill its Contingency Reserve obligations by participating as a member of a Reserve Sharing Group and the Reserve Sharing Group has not provided the same responsibilities and obligations as required of the responsible entity with respect to monitoring and meeting the requirements of Standard BAL-002.
BAL-002-1	R2.	Each Regional Reliability Organization, sub-Regional Reliability	The Regional Reliability	The Regional Reliability	The Regional Reliability	The Regional Reliability

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Organization or Reserve Sharing Group shall specify its Contingency Reserve policies, including:	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 1 of the following sub-requirements.	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 2 or 3 of the following sub-requirements.	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 4 or 5 of the following sub-requirements.	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify all 6 of the following sub-requirements.
BAL-002-1	R2.1.	The minimum reserve requirement for the group.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the minimum reserve requirement for the group.
BAL-002-1	R2.2.	Its allocation among members.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the allocation of reserves among members.
BAL-002-1	R2.3.	The permissible mix of Operating Reserve – Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the permissible mix of Operating Reserve –

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.
BAL-002-1	R2.4.	The procedure for applying Contingency Reserve in practice.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to provide the procedure for applying Contingency Reserve in practice.
BAL-002-1	R2.5.	The limitations, if any, upon the amount of interruptible load that may be included.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the limitations, if any, upon the amount of interruptible load that may be included.
BAL-002-1	R2.6.	The same portion of resource capacity (e.g. reserves from jointly owned generation) shall not be counted more than once as Contingency Reserve by multiple Balancing Authorities.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has allowed the same portion of resource capacity (e.g., reserves from jointly owned generation) to be

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						counted more than once as Contingency Reserve by multiple Balancing Authorities.
BAL-002-1	R3.	Each Balancing Authority or Reserve Sharing Group shall activate sufficient Contingency Reserve to comply with the DCS.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 100% but greater than or equal to 95%.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 95% but greater than or equal to 90%.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 90% but greater than or equal to 85%.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 85%.
BAL-002-1	R3.1.	As a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency. All Balancing Authorities and Reserve Sharing Groups shall review, no less frequently than annually, their probable contingencies to determine their prospective most severe single contingencies.	The Balancing Authority or Reserve Sharing Group failed to review their probable contingencies to determine their prospective most severe single contingencies annually.	N/A	N/A	The Balancing Authority or Reserve Sharing Group failed to carry at least enough Contingency Reserve to cover the most severe single contingency.
BAL-002-1	R4.	A Balancing Authority or Reserve Sharing Group shall meet the Disturbance Recovery Criterion within the Disturbance Recovery Period for 100% of Reportable Disturbances. The Disturbance Recovery Criterion is:	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 90% and less than 100% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 0% and less than or equal to 70% of Reportable Disturbances.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-002-1	R4.1.	A Balancing Authority shall return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to zero. For negative initial ACE values just prior to the Disturbance, the Balancing Authority shall return ACE to its pre-Disturbance value.	N/A	N/A	N/A	The Balancing Authority failed to return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to zero or for negative initial ACE values failed to return ACE to its pre-Disturbance value.
BAL-002-1	R4.2.	The default Disturbance Recovery Period is 15 minutes after the start of a Reportable Disturbance.	N/A	N/A	N/A	N/A
BAL-002-1	R5.	Each Reserve Sharing Group shall comply with the DCS. A Reserve Sharing Group shall be considered in a Reportable Disturbance condition whenever a group member has experienced a Reportable Disturbance and calls for the activation of Contingency Reserves from one or more other group members. (If a group member has experienced a Reportable Disturbance but does not call for reserve activation from other members of the Reserve Sharing Group, then that member shall report as a single Balancing Authority.) Compliance may be demonstrated by either of the following two methods:	The Reserve Sharing Group met the DCS requirement for more than 90% and less than 100% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 0% and less than or equal to 70% of Reportable Disturbances.
BAL-002-1	R5.1.	The Reserve Sharing Group reviews group ACE (or equivalent) and demonstrates compliance to the DCS. To be in compliance, the group ACE (or its equivalent) must meet the	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.				
BAL-002-1	R5.2.	The Reserve Sharing Group reviews each member's ACE in response to the activation of reserves. To be in compliance, a member's ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.	N/A	N/A	N/A	N/A
BAL-002-1	R6.	A Balancing Authority or Reserve Sharing Group shall fully restore its Contingency Reserves within the Contingency Reserve Restoration Period for its Interconnection.	The Balancing Authority or Reserve Sharing Group restored less than 100% but greater than 90% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 90% but greater than 80% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 80% but greater than or equal to 70% of its Contingency Reserve during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than 70% of its Contingency Reserves during the Contingency Reserve Restoration Period.
BAL-002-1	R6.1.	The Contingency Reserve Restoration Period begins at the end of the Disturbance Recovery Period.	N/A	N/A	N/A	N/A
BAL-002-1	R6.2.	The default Contingency Reserve Restoration Period is 90 minutes.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R1.	Each Balancing Authority shall review its Frequency Bias Settings by January 1 of each year and recalculate its setting to reflect any change in the Frequency Response of the Balancing	The Balancing Authority failed to report the method for determining its Frequency Bias	The Balancing Authority failed to report its Frequency Bias Setting to the NERC Operating	The Balancing Authority failed to report its Frequency Bias Settings and the method for	The Balancing Authority failed to review its Frequency Bias Settings by January 1 of each year

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authority Area.	Setting to the NERC Operating Committee. (R1.2)	Committee. (R1.2)	determining that Frequency Bias Setting to the NERC Operating Committee. (R1.2)	and recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.
BAL-003-0.1b	R1.1.	The Balancing Authority may change its Frequency Bias Setting, and the method used to determine the setting, whenever any of the factors used to determine the current bias value change.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R1.2.	Each Balancing Authority shall report its Frequency Bias Setting, and method for determining that setting, to the NERC Operating Committee.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R2.	Each Balancing Authority shall establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways:	N/A	N/A	N/A	The Balancing Authority established and maintained a Frequency Bias Setting that was less than, the Balancing Authority's Frequency Response.
BAL-003-0.1b	R2.1.	The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours.	N/A	N/A	N/A	The Balancing Authority determination of the fixed Frequency Bias value was not based on observations and averaging the Frequency Response from Disturbances during on-peak hours.
BAL-003-0.1b	R2.2.	The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable	N/A	N/A	N/A	The Balancing Authorities variable frequency bias

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by analyzing Frequency Response as it varies with factors such as load, generation, governor characteristics, and frequency.				maintained was not based on analyses of Frequency Response as it varied with factors such as load, generation, governor characteristics, and frequency.
BAL-003-0.1b	R3.	Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.	N/A	N/A	N/A	The Balancing Authority did not operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, during periods when such operation would not have been adverse to system or Interconnection reliability.
BAL-003-0.1b	R4.	Balancing Authorities that use Dynamic Scheduling or Pseudo-ties for jointly owned units shall reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.	N/A	N/A	N/A	The Balancing Authority that used Dynamic Scheduling or Pseudo-ties for jointly owned units did not reflect its respective share of the unit governor droop response in its respective Frequency Bias Setting.
BAL-003-0.1b	R4.1.	Fixed schedules for Jointly Owned Units mandate that Balancing Authority (A) that contains the Jointly Owned Unit must incorporate the respective share of the unit governor droop response for any Balancing	N/A	N/A	N/A	The Balancing Authority (A) that contained the Jointly Owned Unit with fixed schedules did not incorporate the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authorities that have fixed schedules (B and C). See the diagram below.				respective share of the unit governor droop response for any Balancing Authorities that have fixed schedules (B and C).
BAL-003-0.1b	R4.2.	The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit shall not include their share of the governor droop response in their Frequency Bias Setting. ***See Standard for Graphic***	N/A	N/A	N/A	A Balancing Authority that has a fixed schedule (B and C) but does not contain the Jointly Owned Unit included its share of the governor droop response in its Frequency Bias Setting.
BAL-003-0.1b	R5.	Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that served native load failed to have a monthly average Frequency Bias Setting that was at least 1% of the entities estimated yearly peak demand per 0.1 Hz change.
BAL-003-0.1b	R5.1.	Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that does not serve native load did not have a monthly average Frequency Bias Setting that was at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-003-0.1b	R6.	A Balancing Authority that is performing Overlap Regulation Service shall increase its Frequency Bias Setting to match the frequency response of the entire area being controlled. A Balancing Authority shall not change its Frequency Bias Setting when performing Supplemental Regulation Service.	N/A	The Balancing Authority that was performing Overlap Regulation Service changed its Frequency Bias Setting while performing Supplemental Regulation Service.	The Balancing Authority that was performing Overlap Regulation Service failed to increase its Frequency Bias Setting to match the frequency response of the entire area being controlled.	N/A
BAL-004-0	R1.	Only a Reliability Coordinator shall be eligible to act as Interconnection Time Monitor. A single Reliability Coordinator in each Interconnection shall be designated by the NERC Operating Committee to serve as Interconnection Time Monitor.	N/A	N/A	N/A	The responsible entity has designated more than one interconnection time monitor for a single interconnection.
BAL-004-0	R2.	The Interconnection Time Monitor shall monitor Time Error and shall initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.	N/A	N/A	N/A	The responsible entity serving as the Interconnection Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
BAL-004-0	R3.	Each Balancing Authority, when requested, shall participate in a Time Error Correction by one of the following methods:	The Balancing Authority participated in more than 75% and less than 100% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 50% and less than or equal to 75% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 25% and less than or equal to 50% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in less than or equal to 25% of requested Time Error Corrections for the calendar year.
BAL-004-0	R3.1.	The Balancing Authority shall offset its frequency schedule by 0.02 Hertz,	The Balancing Authority failed to	The Balancing Authority failed to	The Balancing Authority failed to	The Balancing Authority failed to

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		leaving the Frequency Bias Setting normal; or	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 0 to 25% of the time error corrections for the year.	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 25 to 50% of the time error corrections for the year.	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 50 to 75% of the time error corrections for the year.	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 75% or more of the time error corrections for the year.
BAL-004-0	R.3.2.	The Balancing Authority shall offset its Net Interchange Schedule (MW) by an amount equal to the computed bias contribution during a 0.02 Hertz Frequency Deviation (i.e. 20% of the Frequency Bias Setting).	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 0 to 25% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 25 to 50% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 50 to 75% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 75% or more of the time error corrections.
BAL-004-0	R4.	Any Reliability Coordinator in an Interconnection shall have the authority to request the Interconnection Time Monitor to terminate a Time Error Correction in progress, or a scheduled Time Error Correction that has not begun, for reliability considerations.	N/A	N/A	N/A	The RC serving as the Interconnection Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
BAL-004-0	R4.1.	Balancing Authorities that have reliability concerns with the execution of a Time Error Correction shall notify their Reliability Coordinator and request the termination of a Time Error Correction in progress.	N/A	N/A	N/A	The Balancing Authority with reliability concerns failed to notify the Reliability Coordinator and request the termination of a Time Error Correction in progress.
BAL-005-0.2b	R1.	All generation, transmission, and load operating within an Interconnection	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		must be included within the metered boundaries of a Balancing Authority Area.				
BAL-005-0.2b	R1.1.	Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Generator Operator with generation facilities operating in an Interconnection failed to ensure that those generation facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.2b	R1.2.	Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Transmission Operator with transmission facilities operating in an Interconnection failed to ensure that those transmission facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.2b	R1.3.	Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Load-Serving Entity with load operating in an Interconnection failed to ensure that those loads were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.2b	R2.	Each Balancing Authority shall maintain Regulating Reserve that can	N/A	N/A	N/A	The Balancing Authority failed to

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
	(Retired)	be controlled by AGC to meet the Control Performance Standard.				maintain Regulating Reserve that can be controlled by AGC to meet Control Performance Standard.
BAL-005-0.2b	R3.	A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to ensure adequate metering, communications, and control equipment was provided.
BAL-005-0.2b	R4.	A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to notify the Host Balancing Authority for whom it is controlling if it was unable to provide the service, as well as any Intermediate Balancing Authorities.
BAL-005-0.2b	R5.	A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.	N/A	N/A	N/A	The Balancing Authority receiving Regulation Service failed to ensure that back-up plans were in place to provide replacement Regulation Service.
BAL-005-0.2b	R6.	The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its	The Balancing Authority failed to calculate ACE as specified in the	N/A	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its inability

Formatted: Font color: Red

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.	inability to calculate ACE.	requirement.		to calculate ACE and failed to use the ACE calculation specified in the requirement in its attempt to calculate ACE.
BAL-005-0.2b	R7.	The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.	N/A	N/A	N/A	The Balancing Authority failed to operate AGC continuously when there were no adverse impacts. OR If its AGC was inoperative the Balancing Authority failed to use manual control to adjust generation to maintain the Net Scheduled Interchange.
BAL-005-0.2b	R8.	The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.	N/A	N/A	N/A	The Balancing Authority failed to ensure that data acquisition for and calculation of ACE occurred at least every six seconds.
BAL-005-0.2b	R8.1.	Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of	N/A	N/A	N/A	The Balancing Authority failed to provide redundant and independent frequency metering equipment that automatically activated upon

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		99.95%.				detection of failure, such that the minimum availability was less than 99.95%.
BAL-005-0.2b	R9.	The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.
BAL-005-0.2b	R9.1.	Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.	N/A	N/A	N/A	The Balancing Authority with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to its Interconnection chose to omit the Interchange Schedule related to the HVDC link from the ACE equation, but failed to model it as internal generation or load.
BAL-005-0.2b	R10.	The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.
BAL-005-0.2b	R11.	Balancing Authorities shall include the effect of Ramp rates, which shall	N/A	N/A	N/A	The Balancing Authority failed to

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.				include the effect of Ramp rates in the Scheduled Interchange values to calculate ACE.
BAL-005-0.2b	R12.	Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.	N/A	N/A	N/A	The Balancing Authority failed to include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.
BAL-005-0.2b	R12.1.	Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.	The Balancing Authority failed to ensure 5% or less of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for 5% or less of the hours.	The Balancing Authority failed to ensure more than 5% up to (and including) 10% of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source. OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for more than 5% up to (and including) 10% of the hours.	The Balancing Authority failed to ensure more than 10% up to (and including) 15% of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source. OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for more than 10% up to (and including) 15% of the hours.	The Balancing Authority failed to ensure more than 15% of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source. OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for more than 15% of the hours.
BAL-005-0.2b	R12.2.	Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are	The responsible entity did not ensure that 5% or less of the power flow and ACE signals are not	The responsible entity did not ensure that more than 5% up to (and including) 10% of the power flow and	The responsible entity did not ensure that more than 10% up to (and including) 15% of the power flow and	The responsible entity did not ensure that more than 15% of the power flow and ACE signals are not filtered

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.	filtered except for Anti-aliasing filtering.	ACE signals are not filtered except for Anti-aliasing filtering.	ACE signals are not filtered except for Anti-aliasing filtering.	except for Anti-aliasing filtering.
BAL-005-0.2b	R12.3.	Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.	N/A	N/A	N/A	The applicable entity did not install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented.
BAL-005-0.2b	R13.	Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.	N/A	N/A	N/A	The Balancing Authority failed to perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment OR the Balancing Authority failed to adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.
BAL-005-0.2b	R14.	The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation	N/A	N/A	N/A	The Balancing Authority failed to provide its operating personnel with sufficient

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.				instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance.
BAL-005-0.2b	R15.	The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.	N/A	N/A	The Balancing Authority failed to periodically test backup power supplies at the Balancing Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.	The Balancing Authority failed to provide adequate and reliable backup power supplies to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.
BAL-005-0.2b	R16.	The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.	The Balancing Authority failed to collect coincident data to the greatest practical extent.	N/A	The Balancing Authority failed to flag missing or bad data for operator display and archival purposes.	The Balancing Authority failed to sample data at least at the same periodicity with which ACE is calculated.
BAL-005-0.2b	R17.	Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices	N/A	N/A	N/A	The Balancing Authority failed to at least annually check

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below: ***See Standard for Values***				and calibrate its time error and frequency devices against a common reference.
BAL-006-2	R1.	Each Balancing Authority shall calculate and record hourly Inadvertent Interchange.	N/A	N/A	N/A	Each Balancing Authority failed to calculate and record hourly Inadvertent Interchange.
BAL-006-2	R2.	Each Balancing Authority shall include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. The Balancing Authority shall take into account interchange served by jointly owned generators.	N/A	N/A	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. OR Failed to take into account interchange served by jointly owned generators.	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. AND Failed to take into account interchange served by jointly owned generators.
BAL-006-2	R3.	Each Balancing Authority shall ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority failed to ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Balancing Authorities.
BAL-006-2	R4.	Adjacent Balancing Authority Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign. Each Balancing Authority shall compute its Inadvertent Interchange based on the following:	The Balancing Authority failed to record Actual Net Interchange values that are equal but opposite in sign to its Adjacent Balancing Authorities.	The Balancing Authority failed to compute Inadvertent Interchange.	The Balancing Authority failed to operate to a common Net Interchange Schedule that is equal but opposite to its Adjacent Balancing Authorities.	N/A
BAL-006-2	R4.1	Each Balancing Authority, by the end of the next business day, shall agree with its Adjacent Balancing Authorities to:	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net Interchanged Schedule. AND The hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-2	R4.1.1.	The hourly values of Net Interchange Schedule.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net Interchanged Schedule.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-006-2	R4.1.2.	The hourly integrated megawatt-hour values of Net Actual Interchange.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-2	R4.2.	Each Balancing Authority shall use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.	N/A	N/A	N/A	The Balancing Authority failed to use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.
BAL-006-2	R4.3.	A Balancing Authority shall make after-the-fact corrections to the agreed-to daily and monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). Changes or corrections based on non-reliability considerations shall not be reflected in the Balancing Authority's Inadvertent Interchange. After-the-fact corrections to scheduled or actual values will not be accepted without agreement of the Adjacent Balancing Authority(ies).	N/A	N/A	N/A	The Balancing Authority failed to make after-the-fact corrections to the agreed-to daily and monthly accounting data to reflect actual operating conditions or changes or corrections based on non-reliability considerations were reflected in the Balancing Authority's Inadvertent Interchange.
BAL-006-2	R5.	Adjacent Balancing Authorities that	Adjacent Balancing	Adjacent Balancing	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cannot mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month shall, for the purposes of dispute resolution, submit a report to their respective Regional Reliability Organization Survey Contact. The report shall describe the nature and the cause of the dispute as well as a process for correcting the discrepancy.	Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities, submitted a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute but failed to provide a process for correcting the discrepancy.	Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month, failed to submit a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute as well as a process for correcting the discrepancy.		
BAL-502-RFC-02	R1.	The Planning Coordinator shall perform and document a Resource Adequacy analysis annually. The Resource Adequacy analysis shall: *[See standard pdf for sub-requirements]*	The Planning Coordinator Resource Adequacy analysis failed to consider 1 or 2 of the Resource availability characteristics subcomponents under R1.4 and documentation of how and why they were included in the analysis or why they were not included OR The Planning	The Planning Coordinator Resource Adequacy analysis failed to express the planning reserve margin developed from R1.1 as a percentage of the net Median forecast peak Load per R1.1.2 OR The Planning Coordinator Resource Adequacy analysis failed to include 1 of the Load forecast Characteristics	The Planning Coordinator Resource Adequacy analysis failed to be performed or verified separately for individual years of Year One through Year Ten per R1.2 OR The Planning Coordinator failed to perform an analysis or verification for one year in the 2 through 5 year period or one year in the 6 though 10 year	The Planning Coordinator failed to perform and document a Resource Adequacy analysis annually per R1. OR The Planning Coordinator Resource Adequacy analysis failed to calculate a Planning reserve margin that will result in the sum of the probabilities for loss of Load for the integrated

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Coordinator Resource Adequacy analysis failed to consider Transmission maintenance outage schedules and document how and why they were included in the analysis or why they were not included per R1.5	subcomponents under R1.3.1 and documentation of its use OR The Planning Coordinator Resource Adequacy analysis failed to include 1 of the Resource Characteristics subcomponents under R1.3.2 and documentation of its use Or The Planning Coordinator Resource Adequacy analysis failed to document that all Load in the Planning Coordinator area is accounted for in its Resource Adequacy analysis per R1.7	period or both per R1.2.2 OR The Planning Coordinator Resource Adequacy analysis failed to include 2 or more of the Load forecast Characteristics subcomponents under R1.3.1 and documentation of their use OR The Planning Coordinator Resource Adequacy analysis failed to include 2 or more of the Resource Characteristics subcomponents under R1.3.2 and documentation of their use OR The Planning Coordinator Resource Adequacy analysis failed to include Transmission	peak hour for all days of each planning year analyzed for each planning period being equal to 0.1 per R1.1 OR The Planning Coordinator failed to perform an analysis for Year One per R1.2.1

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					limitations and documentation of its use per R1.3.3 OR The Planning Coordinator Resource Adequacy analysis failed to include assistance from other interconnected systems and documentation of its use per R1.3.4 OR The Planning Coordinator Resource Adequacy analysis failed to consider 3 or more Resource availability characteristics subcomponents under R1.4 and documentation of how and why they were included in the analysis or why they were not included OR The Planning Coordinator Resource	

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					Adequacy analysis failed to document that capacity resources are appropriately accounted for in its Resource Adequacy analysis per R1.6	
BAL-502-RFC-02	R2.	The Planning Coordinator shall annually document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis. *[See standard pdf for sub-requirements]*	The Planning Coordinator failed to publicly post the documents as specified per requirement R2.1 and R2.2 later than 30 calendar days prior to the beginning of Year One per R2.3	The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis for one of the years in the 2 through 10 year period per R2.1. OR The Planning Coordinator failed to document the Planning Reserve margin calculated per requirement R1.1 for each of the three years in the analysis per R2.2.	The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis for year 1 of the 10 year period per R2.1. OR The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis for two or more of the years in the 2 through 10 year period per R2.1.	The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis per R2.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-001-2a	R1.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.	N/A	N/A	The responsible entity has procedures for the recognition of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection but does not have a procedure for making their operating personnel aware of said events.	The responsible entity failed to have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.
CIP-001-2a	R2.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	N/A	N/A	The responsible entity has demonstrated the existence of a procedure to communicate information concerning sabotage events, but not all of the appropriate parties in the interconnection are identified.	The responsible entity failed to have a procedure for communicating information concerning sabotage events.
CIP-001-2a	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to	N/A	The responsible entity provided its operating personnel with a sabotage response guideline, but failed to include the personnel to contact for reporting disturbances due to	N/A	The responsible entity failed to provide its operating personnel with a sabotage response guideline.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		sabotage events.		sabotage events.		
CIP-001-2a	R4. (Retired)	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	N/A	N/A	The responsible entity has established communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, but has not developed a reporting procedure.	The responsible entity failed to establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, and has not developed a reporting procedure.
CIP-002-3	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
CIP-002-3	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
CIP-002-3	R1.2	The risk-based assessment shall consider the following assets:	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R1.2.1 through R1.2.7 in its risk-based assessment.
CIP-002-3	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.4.	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.7.	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	N/A	N/A	N/A	N/A
CIP-002-3	R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has	The Responsible Entity did not develop a list of its identified Critical

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.			not been reviewed and updated annually as required.	Assets even if such list is null.
CIP-002-3	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null.
CIP-002-3	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-002-4	R1.		N/A	N/A	The Responsible	The Responsible

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.			Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. For the purpose of Standard CIP-002-4, Critical Cyber Assets are	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.				Asset List.
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-3	R1.	Cyber Security Policy — The Responsible Entity shall document and	N/A	N/A	N/A	The Responsible Entity has not

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:				documented or implemented a cyber security policy.
CIP-003-3	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-3	R1.2. (Retired)	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-3	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-3	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		through CIP-009-3.				leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-3	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-3	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-3	R2.3.	Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					are not documented within thirty calendar days of the effective date.	within thirty calendar days of the effective date.
CIP-003-3	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-3	R3. (Retired)	Exceptions — Instances where the Responsible Entity cannot conform to its ~~cyber security policy must be~~ documented as exceptions and authorized by the senior manager or delegate(s).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were not documented.
CIP-003-3	R3.1. (Retired)	Exceptions to the Responsible Entity's cyber security policy must be ~~documented within thirty days of being~~ approved by the senior manager or delegate(s).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).
CIP-003-3	R3.2. (Retired)	Documented exceptions to the cyber security policy must include an ~~explanation as to why the exception is~~ necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-3	R3.3. (Retired)	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed or were not approved on an annual basis by the senior manager or delegate(s) to ensure the exceptions are still required and valid or the review and approval is not documented.
CIP-003-3	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-3	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP- 002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans,	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		incident response plans, and security configuration information.				
CIP-003-3	R4.2. (Retired)	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-3	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-3	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-3	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-3	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, and the information for which they are responsible for authorizing access, but the business phone is missing.	Personnel are not identified by name, title, or the information for which they are responsible for authorizing access.
CIP-003-3	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-3	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						needs and appropriate personnel roles and responsibilities.
CIP-003-3	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-3	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-003-4	R1.	Cyber Security Policy —The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
CIP-003-4	R1.2. (Retired)	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-4	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
CIP-003-4	R2.	Leadership —The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R2.4.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-4	R3. (Retired)	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
CIP-003-4	R3.1. (Retired)	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
CIP-003-4	R3.2. (Retired)	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating	N/A	N/A	The Responsible Entity has a documented exception to the	The Responsible Entity has a documented exception to the

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		measures.			cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-4	R3.3. (Retired)	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
CIP-003-4	R4.	Information Protection —The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-4	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar	N/A	N/A	The information protection program does not include one of the minimum information types to	The information protection program does not include two or more of the minimum

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.			be protected as detailed in R4.1.	information types to be protected as detailed in R4.1.
CIP-003-4	R4.2. (Retired)	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-4	R5.	Access Control —The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	The Responsible Entity implemented but did not document a program for managing access to protected	The Responsible Entity documented but did not implement a program for managing access	The Responsible Entity did not implement nor document a program for managing access

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Critical Cyber Asset information.	to protected Critical Cyber Asset information.	to protected Critical Cyber Asset information.
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-4	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		roles and responsibilities.				privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-4	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	The Responsible Entity has established but not documented a change control process OR The Responsible Entity has established but not documented a configuration management process.	The Responsible Entity has established but not documented both a change control process and configuration management process.	The Responsible Entity has not established and documented a change control process OR The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a change control process AND The Responsible Entity has not established and documented a configuration management process.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-3	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	N/A	N/A	The Responsible[1] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
CIP-004-3	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be	N/A	N/A	The Responsible[2] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		updated whenever necessary.				physical access to Critical Cyber Assets.
CIP-004-3	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A	N/A	N/A	Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-3	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-3	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-3	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but	The Responsible Entity did not maintain documentation that training is conducted

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					did not include attendance records.	at least annually, including the date the training was completed and attendance records.
CIP-004-3	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R3, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, as stated in R3, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-004-3	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		criticality of the position.			in the U.S.) or a seven-year criminal check.	in the U.S.) and seven-year criminal check.
CIP-004-3	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-3	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-3	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 15% or more of the authorized personnel.
CIP-004-3	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-3	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						longer require such access to Critical Cyber Assets.
CIP-004-4	R1.	Awareness —The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g., emails, memos, computer based training, etc.); • Indirect communications (e.g., posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
CIP-004-4	R2.	Training —The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to	The Responsible Entity did not establish, document, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access to Critical Cyber Assets.		Critical Cyber Assets.	Critical Cyber Assets.
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-4	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.
CIP-004-4	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	such personnel were granted such access except in specified circumstances such as an emergency.	existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-4	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				update it for cause when applicable.	after the initial personnel risk assessment.	assessment nor was it updated for cause when applicable.
CIP-004-4	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.
CIP-004-4	R4.	Access —The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets,	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 10% or more	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 15% or more

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			missing at least one individual but less than 5% of the authorized personnel.		but less than 15% of the authorized personnel.	of the authorized personnel.
CIP-004-4	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-4	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-3a	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-3a	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-3a	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the dial-up device.
CIP-005-3a	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-3a	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-3a	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-	N/A	N/A	N/A	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded one (1) or more of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		009-3.				Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3c Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.
CIP-005-3a	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of one or more of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
CIP-005-3a	R2.	Electronic Access Controls — The Responsible Entity shall implement and	N/A	N/A	N/A	The Responsible Entity did not

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).				implement or did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005-3a	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-3a	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	N/A	N/A	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						services.
CIP-005-3a	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-3a	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-3a	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-3a	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-3a	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-3a	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		004-3 Requirement R4.				
CIP-005-3a	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-3a	R2.6. (Retired)	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
CIP-005-3a	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-3a	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						monitoring at one or more access points to dial-up devices.
CIP-005-3a	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR The above alerts do not provide for appropriate notification to designated response personnel. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
CIP-005-3a	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerability assessment shall include, at a minimum, the following:				annually for one or more of the access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-3a	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-005-3a	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			5% of the documentation to support compliance with the requirements of Standard CIP-005.	documentation to support compliance with the requirements of Standard CIP-005.	documentation to support compliance with the requirements of Standard CIP-005.	with the requirements of Standard CIP-005.
CIP-005-3a	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-3a	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-3a	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-005-4a	R1.	Electronic Security Perimeter —The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and	The Responsible Entity did not document one or more access points to the Electronic	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Security Perimeter(s).		an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
CIP-005-4a	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-4a	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
CIP-005-4a	R1.3.	Communication links connecting	N/A	N/A	N/A	At least one end point

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).				of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-4a	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-4a	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
CIP-005-4a	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-4a	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005-4a	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-4a	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document,	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document,

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Perimeter.	individually or by specified grouping, the configuration of those ports and services.	individually or by specified grouping, the configuration of those ports and services.
CIP-005-4a	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-4a	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-4a	R2.5.	The required documentation shall, at least, identify and describe:	The required documentation for R2 did not include one of the elements described in R2.5.1 through	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			R2.5.4			
CIP-005-4a	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.6. (Retired)	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			appropriate use banner on the user screen upon all interactive access attempts.			
CIP-005-4a	R3.	Monitoring Electronic Access —The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
CIP-005-4a	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			manual processes for monitoring at less than 5% of the access points to dial-up devices.			
CIP-005-4a	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate notification to designated response personnel.	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
CIP-005-4a	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-4a	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-005-4a	R5.	Documentation Review and Maintenance —The Responsible Entity shall review, update, and maintain all documentation to support compliance with the	The Responsible Entity did not review, update, and maintain at	The Responsible Entity did not review, update, and maintain greater than 5% but	The Responsible Entity did not review, update, and maintain greater than 10% but	The Responsible Entity did not review, update, and maintain greater than 15% of

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		requirements of Standard CIP-005-4a.	least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	the documentation to support compliance with the requirements of Standard CIP-005-4.
CIP-005-4a	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
CIP-005-4a	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
CIP-005-4a	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable	The Responsible Entity retained electronic access	The Responsible Entity retained electronic access logs	The Responsible Entity retained electronic access logs	The Responsible Entity retained electronic access logs

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	logs for 75 or more calendar days, but for less than 90 calendar days.	for 60 or more calendar days, but for less than 75 calendar days.	for 45 or more calendar days , but for less than 60 calendar days.	for less than 45 calendar days.
CIP-006-3c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
CIP-006-3c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall")

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						border cannot be established, the Responsible Entity has not deployed or documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-3c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter or does not identify measures to control entry at those access points.
CIP-006-3c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-3c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-3c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the review of access authorization requests or the revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
CIP-006-3c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A	N/A	N/A	The Responsible Entity did not include or implement a visitor control program in its physical security plan or it does not meet the requirements of continuous escort.
CIP-006-3c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-3c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-3c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address r updating the physical security plan within thirty calendar days of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access controls, monitoring controls, or logging controls.				completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration
CIP-006-3c	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-3c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A	N/A	N/A	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was not afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
CIP-006-3c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-3c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	N/A	N/A	N/A	N/A
CIP-006-3c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) does not reside within an identified Physical Security Perimeter.
CIP-006-3c	R4	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the	N/A	N/A	N/A	The Responsible Entity has not documented or has not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets				more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-3c	R5	Monitoring Physical Access — The Responsible Entity shall document and	N/A	N/A.	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.				Entity has not documented or has not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-3.
CIP-006-3c	R6	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of		N/A	N/A	The Responsible Entity has not implemented or has not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4				control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-3c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	N/A	N/A	N/A	The responsible entity did not retain physical access logs for at least ninety calendar days.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-3c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-3c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-3c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-3c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.	Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR	The Responsible Entity did not document, implement, and maintain a physical security plan.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity created and implemented but did not maintain a physical security plan.	
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Security Perimeter.	entry at those access points.	entry at those access points.
CIP-006-4c	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-4c	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-4c	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.
CIP-006-4c	R1.6.	A visitor control program for visitors (personnel without authorized unescorted	The responsible Entity included a	The responsible Entity included a visitor	The responsible Entity included a	The Responsible Entity did not include

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access to a Physical Security Perimeter), containing at a minimum the following:	visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.	control program in its physical security plan, but either did not log the visitor or did not log the escort.	visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	or implement a visitor control program in its physical security plan.
CIP-006-4c	R1.6.1.	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.6.2.	Continuous escorted access of visitors within the Physical Security Perimeter.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or reconfiguration.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					reconfiguration.	
CIP-006-4c	R1.8.	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical Security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-4c	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP- 009-4.		Standard CIP-009-4.	point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	N/A	N/A	N/A	N/A
CIP-006-4c	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						an identified Physical Security Perimeter.
CIP-006-4c	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. Security Personnel: Personnel responsible for controlling	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel:	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets..
CIP-006-4c	R5.	Monitoring Physical Access —The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access points by authorized personnel as specified in Requirement R4.		personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-4.
CIP-006-4c	R6.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week..	control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
CIP-006-4c	R7.	Access Log Retention —The Responsible Entity shall retain physical access logs for at least ninety calendar	The Responsible Entity retained physical access	The Responsible Entity retained physical access logs	The Responsible Entity retained physical access logs	The Responsible Entity retained physical access logs

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	logs for 75 or more calendar days, but for less than 90 calendar days.	for 60 or more calendar days, but for less than 75 calendar days.	for 45 or more calendar days, but for less than 60 calendar days.	for less than 45 calendar days.
CIP-006-4c	R8.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
CIP-006-4c	R8.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-3	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	N/A	N/A	N/A	The Responsible Entity did not ensure the prevention of adverse affects described in R1, by not including the required minimum significant changes. OR The Responsible Entity did not address one or more of the following: R1.1, R1.2, R1.3.
CIP-007-3	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	N/A	N/A	N/A	N/A
CIP-007-3	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-3	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-3	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-3	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk.
CIP-007-3	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document, either separately or as a component of the

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).				documented configuration management process specified in CIP-003-3 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-3	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-3	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk.
CIP-007-3	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-3	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-3	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	N/A	N/A	N/A	The Responsible Entity did not document or did not implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-3	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	N/A	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-3	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						know" with respect to work functions performed.
CIP-007-3	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-3	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-3	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
CIP-007-3	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.				implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-3	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-3	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-3	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity has not implemented (one or more components of) a policy for managing the use of such accounts that limits

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-3	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity does not require passwords subject to R5.3.1, R5.3.2, R5.3.3. OR Does not use passwords subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-3	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-3	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-3	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-3	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to	N/A	N/A	N/A	The Responsible Entity as technically feasible, did not implement automated tools or organizational

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitor system events that are related to cyber security.				process controls, to monitor system events that are related to cyber security on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
CIP-007-3	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-3	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						incident response as required in Standard CIP-008.
CIP-007-3	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-3	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-3	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.	N/A	N/A	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005- 3 but did not address redeployment as specified in R7.2.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3. OR

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1. ~~OR~~ ~~The Responsible Entity did not maintain records pertaining to disposal or[3] redeployment as specified in R7.3.~~

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						(Deleted text retired)
CIP-007-3	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-3	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-3	R7.3. (Retired)	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-3	R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment on one or more Cyber Assets within the Electronic Security Perimeter at least annually. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
CIP-007-3	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-3	R8.2.	A review to verify that only ports and services required for operation of the	N/A	N/A	N/A	N/A

Formatted: Font color: Red

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Cyber Assets within the Electronic Security Perimeter are enabled;				
CIP-007-3	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-3	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-007-3	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 at least annually and changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.
CIP-007-4	R1.	Test Procedures —The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not	N/A	The Responsible Entity did create, implement and maintain the test procedures as required	The Responsible Entity did not create, implement and maintain the test procedures as	The Responsible Entity did not create, implement and maintain the test procedures as

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.		in R1.1, but did not document that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	required in R1.1.	required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
CIP-007-4	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	N/A	N/A	N/A	N/A
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-4	R2.	Ports and Services —The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Entity did not document compensating measure(s) applied to mitigate risk exposure.
CIP-007-4	R3.	Security Patch Management —The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within	The Responsible Entity documented the assessment of	The Responsible Entity documented the assessment of security	The Responsible Entity documented the assessment of	The Responsible Entity documented the assessment of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		thirty calendar days of availability of the patches or upgrades.	security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.
CIP-007-4	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
CIP-007-4	R4.	Malicious Software Prevention —The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware")	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Security Perimeter(s).	prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-4	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	The Responsible Entity, as technically feasible, documented and implemented a	The Responsible Entity, as technically feasible, did not document but implemented a process, including	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-4	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-4	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.	At least one user account but less than 1% of user accounts	One (1) % or more of user accounts but less than 3% of user accounts implemented	Three (3) % or more of user accounts but less than 5% of user accounts	Five (5) % or more of user accounts implemented by the Responsible Entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			implemented by the Responsible Entity, were not approved by designated personnel.	by the Responsible Entity were not approved by designated personnel.	implemented by the Responsible Entity were not approved by designated personnel.	were not approved by designated personnel.
CIP-007-4	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
CIP-007-4	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						account privileges including factory default accounts.
CIP-007-4	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-4	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization,	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization,	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		risk.				
CIP-007-4	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-4	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 but did not maintain records as specified in R7.3. (Retired)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
CIP-007-4	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-4	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R7.3. (Retired)	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-4	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-4	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	N/A	N/A	N/A	N/A
CIP-007-4	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A

Formatted: Font color: Red

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-007-4	R9.	Documentation Review and Maintenance —The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.
CIP-008-3	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					components.	Cyber Security Incident.
CIP-008-3	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-3	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-3	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	N/A	N/A	N/A	N/A
CIP-008-3	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	N/A	N/A	N/A	N/A
CIP-008-3	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-3	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-3	R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		years.				Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-008-4	R1.	Cyber Security Incident Response Plan —The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-4	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	N/A	N/A	N/A	N/A
CIP-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		calendar days of any changes.				
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-4	R2.	Cyber Security Incident Documentation —The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for two but less than three calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than two calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than one calendar year.	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1.
CIP-009-3	R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	N/A	N/A	N/A	The Responsible Entity has not created or has not annually reviewed their recovery plan(s) for Critical Cyber Assets OR has created a plan but did not address one or more of the requirements CIP-

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						009-1 R1.1 and R1.2.
CIP-009-3	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-3	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-3	R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-3	R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were not communicated to

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change.
CIP-009-3	R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-3	R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.
CIP-009-4	R1.	Recovery Plans —The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	N/A	The Responsible Entity has not annually reviewed recovery plan(s) for Critical Cyber Assets.	The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP-009-4 R1.1 or R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-4 R1.1 and R1.2.
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the recovery plan(s).				
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-4	R2.	Exercises —The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-4	R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementation of the recovery plan(s) in more than 180 calendar days of the change.
CIP-009-4	R4.	Backup and Restore —The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-4	R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
COM-001-1.1	R1.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:	N/A	The responsible entity failed to provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information to one of the groups specified in R1.1, or R1.2, or R1.3	The responsible entity failed to provide adequate and reliable telecommunications facilities for the exchange of Interconnection or operating information to two of the groups specified in R1.1, or R1.2, or R1.3.	The responsible entity failed to provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information to all 3 of the groups specified in R1.1, or R1.2, or R1.3. OR The responsible entity's telecommunications is not redundant or diversely routed as applicable as specified in R1.4
COM-001-1.1	R1.1.	Internally.	N/A	N/A	N/A	N/A
COM-001-1.1	R1.2.	Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	N/A
COM-001-1.1	R1.3.	With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.	N/A	N/A	N/A	N/A
COM-001-1.1	R1.4.	Where applicable, these facilities shall be redundant and diversely routed.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
COM-001-1.1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.	N/A	The responsible entity failed to give special attention to emergency telecommunications facilities and equipment not used for routine communications.	N/A	The responsible entity failed to manage, alarm, test and/or actively monitor its vital telecommunications facilities.
COM-001-1.1	R3.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.	N/A	N/A	The responsible entity failed to assist in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.	The responsible entity failed to provide a means to coordinate telecommunications among their respective areas including assisting in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.
COM-001-1.1	R4.	Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing Authorities may use an alternate language for internal operations.	N/A	N/A	N/A	The responsible entity used a language other than English and failed to have an agreement to do so.
COM-001-	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing	N/A	N/A	N/A	The responsible entity did not have

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
1.1		Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.				written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.
COM-001-1.1	R6.	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, “NERCNet Security Policy.”	The NERCNet User Organization failed to adhere to 5% or less of the requirements listed in Attachment 1-COM-001, , "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to more than 5% up to (and including) 10% of the requirements listed in Attachment 1 - COM-001, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to more than 10% up to (and including) 15% of the requirements listed in Attachment 1-COM-001 "NERCNet Security Policy".	The NERCNet User Organization failed to more than 15% of the requirements listed in Attachment 1-COM-001, "NERCNet Security Policy".
COM-002-2	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.	N/A	The responsible entity did not have data links with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. OR The responsible entity did not have voice links with appropriate Reliability Coordinators, Balancing Authorities, and	N/A	The responsible entity failed to have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. OR The responsible entity's communications were not staffed and available for addressing real time emergency

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Transmission Operators.		conditions.
COM-002-2	R1.1.	Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.	N/A	N/A	The responsible entity failed to notify all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding was anticipated.	The responsible entity failed to notify its Reliability Coordinator through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding was anticipated.
COM-002-2	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall issue directives in a clear, concise, and definitive manner; shall ensure the recipient of the directive repeats the information back correctly; and shall acknowledge the response as correct or repeat the original statement to resolve any misunderstandings.	N/A	The responsible entity provided a clear directive in a clear, concise and definitive manner and required the recipient to repeat the directive, but did not acknowledge the recipient was correct in the repeated directive.	The responsible entity provided a clear directive in a clear, concise and definitive manner, but did not require the recipient to repeat the directive.	The responsible entity failed to provide a clear directive in a clear, concise and definitive manner when required.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-001-0.1b	R1.	Balancing Authorities shall have operating agreements with adjacent Balancing Authorities that shall, at a minimum, contain provisions for emergency assistance, including provisions to obtain emergency assistance from remote Balancing Authorities.	N/A	The Balancing Authority demonstrated the existence of an operating agreement with at least one adjacent Balancing Authority for emergency assistance, but the agreement did not include provision for obtaining emergency assistance from any remote Balancing Authority.	N/A	The Balancing Authority did not demonstrate the existence of any operating agreements with adjacent Balancing Authorities that include provision for emergency assistance with adjacent Balancing Authorities.
EOP-001-0.1b	R2.	The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. The plan shall include the details on how the Transmission Operator will implement load reduction in sufficient amount and time to mitigate the IROL violation before system separation or collapse would occur. The load reduction plan must be capable of being implemented within 30 minutes.	N/A	N/A	The Transmission Operator demonstrated the existence of an emergency load reduction plan for each identified IROL but at least one of the plans will take longer than 30 minutes to implement.	The Transmission Operator failed to demonstrate the existence of an emergency load reduction plan for all identified IROLs.
EOP-001-0.1b	R3.	Each Transmission Operator and Balancing Authority shall:	N/A	N/A	N/A	N/A
EOP-001-0.1b	R3.1.	Develop, maintain, and implement a set of plans to mitigate operating emergencies for insufficient generating capacity.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating emergencies for insufficient	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans to mitigate operating emergencies

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				emergencies for insufficient generating capacity and the plans are implemented but the plans are not maintained.	generating capacity but the plans are neither maintained nor implemented.	for insufficient generating capacity.
EOP-001-0.1b	R3.2.	Develop, maintain, and implement a set of plans to mitigate operating emergencies on the transmission system.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating emergencies on the transmission system and the plans are implemented but the plans are not maintained.	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating emergencies on the transmission system but the plans are neither maintained nor implemented.	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans to mitigate operating emergencies on the transmission system.
EOP-001-0.1b	R3.3.	Develop, maintain, and implement a set of plans for load shedding.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for load shedding and the plans are implemented but the plans are not maintained.	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for load shedding but the plans are neither maintained nor implemented.	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans for load shedding.
EOP-001-0.1b	R3.4.	Develop, maintain, and implement a set of plans for system restoration.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for system restoration and the	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for system restoration but the plans are neither maintained	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans for system restoration.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				plans are implemented but the plans are not maintained.	nor implemented.	
EOP-001-0.1b	R4.	Each Transmission Operator and Balancing Authority shall have emergency plans that will enable it to mitigate operating emergencies. At a minimum, Transmission Operator and Balancing Authority emergency plans shall include:	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans do not include sub-requirement R4.4.	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans do not include sub-requirement R4.3.	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans do not include either sub-requirement R4.1 or R4.2.	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans are missing two (2) or more of the sub-requirements identified for R4.
EOP-001-0.1b	R4.1.	Communications protocols to be used during emergencies.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R4.2.	A list of controlling actions to resolve the emergency. Load reduction, in sufficient quantity to resolve the emergency within NERC-established timelines, shall be one of the controlling actions.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R4.3.	The tasks to be coordinated with and among adjacent Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R4.4.	Staffing levels for the emergency.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R5.	Each Transmission Operator and Balancing Authority shall include the applicable elements in Attachment 1-EOP-001 when developing an emergency plan.	The Transmission Operator and Balancing Authority emergency plan has complied with 90% or more of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 70% to 90% of the number of sub-	The Transmission Operator and Balancing Authority emergency plan has complied with between 50% to 70% of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 50% or less of the number of sub-components

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				components.		
EOP-001-0.1b	R6.	The Transmission Operator and Balancing Authority shall annually review and update each emergency plan. The Transmission Operator and Balancing Authority shall provide a copy of its updated emergency plans to its Reliability Coordinator and to neighboring Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to provide evidence that it completed an annual review, and updated each of its emergency plans appropriately. OR The Transmission Operator or Balancing Authority failed to provide a copy of one of its updated emergency plans to its Reliability Coordinator, all its neighboring Transmission Operators, and all its neighboring Balancing Authorities.
EOP-001-0.1b	R7.	The Transmission Operator and Balancing Authority shall coordinate its emergency plans with other Transmission Operators and Balancing Authorities as appropriate. This coordination includes the following steps, as applicable:	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in R7.4 was applicable and was not included.	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in R7.3 was applicable and	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in either R7.1 or R7.2 was applicable and was not included. .	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in two (2) or more of the sub-requirements was applicable and was not included.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				was not included.		
EOP-001-0.1b	R7.1.	The Transmission Operator and Balancing Authority shall establish and maintain reliable communications between interconnected systems.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R7.2.	The Transmission Operator and Balancing Authority shall arrange new interchange agreements to provide for emergency capacity or energy transfers if existing agreements cannot be used.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R7.3.	The Transmission Operator and Balancing Authority shall coordinate transmission and generator maintenance schedules to maximize capacity or conserve the fuel in short supply. (This includes water for hydro generators.)	N/A	N/A	N/A	N/A
EOP-001-0.1b	R7.4.	The Transmission Operator and Balancing Authority shall arrange deliveries of electrical energy or fuel from remote systems through normal operating channels.	N/A	N/A	N/A	N/A
EOP-002-3.1	R1.	Each Balancing Authority and Reliability Coordinator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area and shall exercise specific authority to alleviate capacity and energy emergencies.	N/A	N/A	N/A	The Balancing Authority or Reliability Coordinator does not have responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area OR The Balancing Authority or Reliability Coordinator did not exercise its authority

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						to alleviate capacity and energy emergencies.
EOP-002-3.1	R2.	Each Balancing Authority shall, when required and as appropriate, take one or more actions as described in its capacity and energy emergency plan, to reduce risks to the interconnected system.	N/A	N/A	N/A	The Balancing Authority did not implement its capacity and energy emergency plan, when required and as appropriate, to reduce risks to the interconnected system.
EOP-002-3.1	R3.	A Balancing Authority that is experiencing an operating capacity or energy emergency shall communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.	N/A	N/A	The Balancing Authority communicated its current and future system conditions to its Reliability Coordinator but did not communicate to one or more of its neighboring Balancing Authorities.	The Balancing Authority has failed to communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.
EOP-002-3.1	R4.	A Balancing Authority anticipating an operating capacity or energy emergency shall perform all actions necessary including bringing on all available generation, postponing equipment maintenance, scheduling interchange purchases in advance, and being prepared to reduce firm load.	N/A	N/A	N/A	The Balancing Authority has failed to perform the necessary actions as required and stated in the requirement.
EOP-002-3.1	R5.	A deficient Balancing Authority shall only use the assistance provided by the Interconnection's frequency bias for the time needed to implement corrective actions. The Balancing Authority shall not unilaterally adjust generation in an attempt to return Interconnection frequency to	N/A	N/A	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement corrective	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		normal beyond that supplied through frequency bias action and Interchange Schedule changes. Such unilateral adjustment may overload transmission facilities.			actions.	corrective actions and unilaterally adjust generation in an attempt to return Interconnection frequency to normal beyond that supplied through frequency bias action and Interchange Schedule changes.
EOP-002-3.1	R6.	If the Balancing Authority cannot comply with the Control Performance and Disturbance Control Standards, then it shall immediately implement remedies to do so. These remedies include, but are not limited to:	The Balancing Authority failed to comply with one of the sub-components.	The Balancing Authority failed to comply with 2 of the sub-components.	The Balancing Authority failed to comply with 3 of the sub-components.	The Balancing Authority failed to comply with more than 3 of the sub-components.
EOP-002-3.1	R6.1.	Loading all available generating capacity.	N/A	N/A	N/A	The Balancing Authority did not use all available generating capacity.
EOP-002-3.1	R6.2.	Deploying all available operating reserve	N/A	N/A	N/A	The Balancing Authority did not deploy all of its available operating reserve.
EOP-002-3.1	R6.3.	Interrupting interruptible load and exports.	N/A	N/A	N/A	The Balancing Authority did not interrupt interruptible load and exports.
EOP-002-3.1	R6.4.	Requesting emergency assistance from other Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority did not request emergency assistance from other Balancing Authorities.
EOP-002-3.1	R6.5.	Declaring an Energy Emergency through its	N/A	N/A	N/A	The Balancing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinator; and				Authority did not declare an Energy Emergency through its Reliability Coordinator.
EOP-002-3.1	R6.6.	Reducing load, through procedures such as public appeals, voltage reductions, curtailing interruptible loads and firm loads.	N/A	N/A	N/A	The Balancing Authority did not implement one or more of the procedures stated in the requirement.
EOP-002-3.1	R7.	Once the Balancing Authority has exhausted the steps listed in Requirement 6, or if these steps cannot be completed in sufficient time to resolve the emergency condition, the Balancing Authority shall:	N/A	N/A	The Balancing Authority has met only one of the two requirements	The Balancing Authority has not met either of the two requirements
EOP-002-3.1	R7.1.	Manually shed firm load without delay to return its ACE to zero; and	N/A	N/A	N/A	The Balancing Authority did not manually shed firm load without delay to return it's ACE to zero.
EOP-002-3.1	R7.2.	Request the Reliability Coordinator to declare an Energy Emergency Alert in accordance with Attachment 1-EOP-002 "Energy Emergency Alerts."	The Balancing Authority's implementation of an Energy Emergency Alert has missed minor program/procedural elements in Attachment 1-EOP-002-0.	N/A	N/A	The Balancing Authority has failed to meet one or more of the requirements of Attachment 1-EOP-002-0.
EOP-002-3.1	R8.	A Reliability Coordinator that has any Balancing Authority within its Reliability Coordinator area experiencing a potential or actual Energy Emergency shall initiate an Energy Emergency Alert as detailed in	The Reliability Coordinator's implementation of an Energy Emergency Alert has missed	N/A	N/A	The Reliability Coordinator has failed to meet one or more of the requirements of Attachment 1-EOP-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1-EOP-002 "Energy Emergency Alerts." The Reliability Coordinator shall act to mitigate the emergency condition, including a request for emergency assistance if required.	minor program/procedural elements in Attachment 1-EOP-002-0.			002-0.
EOP-002-3.1	R9.	When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources) as permitted in its transmission tariff:	The Reliability Coordinator failed to comply with one (1) of the sub-components.	The Reliability Coordinator failed to comply with two (2) of the sub-components.	The Reliability Coordinator has failed to comply with three (3) of the sub-components.	The Reliability Coordinator has failed to comply with all four (4) of the sub-components.
EOP-002-3.1	R9.1.	The deficient Load-Serving Entity shall request its Reliability Coordinator to initiate an Energy Emergency Alert in accordance with Attachment 1-EOP-002 "Energy Emergency Alerts."	N/A	N/A	N/A	The Load-Serving Entity failed to request its Reliability Coordinator to initiate an Energy Emergency Alert.
EOP-002-3.1	R9.2.	The Reliability Coordinator shall submit the report to NERC for posting on the NERC Website, noting the expected total MW that may have its transmission service priority changed.	N/A	N/A	N/A	The Reliability Coordinator has failed to report to NERC as directed in the requirement.
EOP-002-3.1	R9.3.	The Reliability Coordinator shall use EEA 1 to forecast the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.	N/A	N/A	N/A	The Reliability Coordinator failed to use EEA 1 to forecast the change of the priority of transmission service as directed in the requirement.
EOP-002-3.1	R9.4.	The Reliability Coordinator shall use EEA 2 to announce the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to	N/A	N/A	N/A	The Reliability Coordinator failed to use EEA 2 to announce the change

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Priority 7.				of the priority of transmission service as directed in the requirement.
EOP-003-1	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed customer load.
EOP-003-1	R2.	Each Transmission Operator and Balancing Authority shall establish plans for automatic load shedding for underfrequency or undervoltage conditions.	N/A	N/A	N/A	The responsible entity did not establish plans for automatic load shedding as directed by the requirement.
EOP-003-1	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans among other interconnected Transmission Operators and Balancing Authorities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting 5% or less of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 5% up to (and including) 10% of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 10%, up to (and including) 15% or less, of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 15% of its required entities.
EOP-003-1	R4.	A Transmission Operator or Balancing Authority shall consider one or more of these factors in designing an automatic load shedding scheme: frequency, rate of frequency decay, voltage level, rate of voltage decay, or power flow levels.	N/A	N/A	N/A	The applicable entity did not consider one of the five required elements, as directed by the requirement.
EOP-003-1	R5.	A Transmission Operator or Balancing Authority shall implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to implement load shedding in steps

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.
EOP-003-1	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed additional load after it had separated from the Interconnection when there was insufficient generating capacity to restore system frequency following automatic underfrequency load shedding.
EOP-003-1	R7.	The Transmission Operator and Balancing Authority shall coordinate automatic load shedding throughout their areas with underfrequency isolation of generating units, tripping of shunt capacitors, and other automatic actions that will occur under abnormal frequency, voltage, or power flow conditions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 5% or less of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting between 5 - 10% of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 10-15%, inclusive, of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting greater than 15% of its automatic actions.
EOP-003-1	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator-controlled manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be capable of implementing the load shedding in a timeframe adequate for responding to the emergency.	N/A	The responsible entity did not have plans for operator controlled manual load shedding, as directed by the requirement.	The responsible entity has plans for manual load shedding but did not have the capability to implement the load shedding, as directed by the requirement.	The responsible entity did not have plans for operator controlled manual load shedding, as directed by the requirement nor had the capability to implement the load shedding, as directed by the requirement.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-003-2	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed customer load.
EOP-003-2	R2.	Each Transmission Operator shall establish plans for automatic load shedding for undervoltage conditions if the Transmission Operator or its associated Transmission Planner(s) or Planning Coordinator(s) determine that an under-voltage load shedding scheme is required.	N/A	N/A	N/A	The Transmission Operator did not establish plans for automatic load shedding for undervoltage conditions as directed by the requirement.
EOP-003-2	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans, excluding automatic under-frequency load shedding plans, among other interconnected Transmission Operators and Balancing Authorities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting 5% or less of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 5% up to (and including) 10% of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 10%, up to (and including) 15% or less, of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 15% of its required entities.
EOP-003-2	R4.	A Transmission Operator shall consider one or more of these factors in designing an automatic under voltage load shedding scheme: voltage level, rate of voltage decay, or power flow levels.	N/A	N/A	N/A	The Transmission Operator failed to consider at least one of the three elements voltage level, rate of voltage decay, or power flow levels) listed in the requirement.
EOP-003-2	R5.	A Transmission Operator or Balancing Authority shall implement load shedding, excluding automatic under-frequency load	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shedding, in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.				implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.
EOP-003-2	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed additional load after it had separated from the Interconnection when there was insufficient generating capacity to restore system frequency following automatic underfrequency load shedding.
EOP-003-2	R7.	The Transmission Operator shall coordinate automatic undervoltage load shedding throughout their areas with tripping of shunt capacitors, and other automatic actions that will occur under abnormal voltage, or power flow conditions.	The Transmission Operator did not coordinate automatic undervoltage load shedding with 5% or less of the types of automatic actions described in the Requirement.	The Transmission Operator did not coordinate automatic undervoltage load shedding with more than 5% up to (and including) 10% of the types of automatic actions described in the Requirement.	The Transmission Operator did not coordinate automatic undervoltage load shedding with more than 10% up to (and including) 15% of the types of automatic actions described in the Requirement.	The Transmission Operator did not coordinate automatic undervoltage load shedding with more than 15% of the types of automatic actions described in the Requirement.
EOP-003-2	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator controlled manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be	N/A	The responsible entity did not have plans for operator controlled manual load shedding, as	The responsible entity has plans for manual load shedding but did not have the capability to implement the load	The responsible entity did not have plans for operator controlled manual load shedding, as directed by the

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		capable of implementing the load shedding in a timeframe adequate for responding to the emergency.		directed by the requirement.	shedding, as directed by the requirement.	requirement nor had the capability to implement the load shedding, as directed by the requirement.
EOP-004-1	R1. (Retired)	Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	The Regional Reliability Organization has demonstrated the existence of a regional reporting procedure, but the procedure is missing minor details or minor program/procedural elements.	The Regional Reliability Organization Regional reporting procedure have been is missing one element that would make the procedure meet the requirement.	The Regional Reliability Organization Regional has a regional reporting procedure but the procedure is not current.	The Regional Reliability Organization does not have a regional reporting procedure.
EOP-004-1	R2.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	The responsible entity failed to promptly analyze 5% or less of its disturbances on the BES.	The responsible entity failed to promptly analyze more than 5% up to (and including) 10% of its disturbances on the BES.	The responsible entity failed to promptly analyze more than 10% up to (and including) 15% of its disturbances on the BES.	The responsible entity failed to promptly analyze more than 15% of its disturbances on the BES.
EOP-004-1	R3.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	N/A	N/A	N/A	The responsible entities failed to provide a preliminary written report as directed by the requirement.
EOP-004-1	R3.1.	The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a	The responsible entity submitted the report as required in R3.1 more than 24 but less than or equal to 36 hours after the disturbance or unusual occurrence,	The responsible entity submitted the report as required in R3.1 more than 36 hours but less than or equal to 48 hours after the disturbance	The responsible entities submitted the report as required in R3.1 more than 48 hours but less than or equal to 72 hours after the disturbance or unusual	The responsible entities submitted the report as required in R3.1 more than 72-hours after the disturbance or unusual occurrence or

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.	or discovery of the disturbance or unusual occurrence.	or unusual occurrence, or discovery of the disturbance or unusual occurrence.	occurrence, or discovery of the disturbance or unusual occurrence.	discovery of the disturbance or unusual occurrence.
EOP-004-1	R3.2.	Applicable reporting forms are provided in Attachments 022-1 and 022-2.	N/A	N/A	N/A	N/A
EOP-004-1	R3.3.	Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	N/A	N/A	N/A	The responsible entity did not provide its Regional Reliability Organization(s) and NERC with verbal notification or updates about a disturbance as specified in R3.3.
EOP-004-1	R3.4.	If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this	The responsible entity submitted the final report no more than 30 days past the 60 day due date; or the final report was missing one of the three elements specified in R3.4.	The responsible entity submitted the final report between 31 days and 60 days inclusive past the 60 day due date. OR The final report was missing two of the	The responsible entity submitted the final report between 61 days and 90 days inclusive past the 60 day due date	The responsible entity failed to submit the final report. OR The responsible entity submitted the final report 91 days or more past the 60 day due date

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.		three elements specified in R3.4.		OR The responsible entity submitted a final report that was missing all three of the elements specified in R3.4.
EOP-004-1	R4.	When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	N/A	N/A	N/A	The RRO did not make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.
EOP-004-1	R5.	The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.	The Regional Reliability Organization reviewed all final report recommendations less than twice a year.	The Regional Reliability Organization reviewed 75% or more final report recommendations twice a year.	The Regional Reliability Organization has not reported on any recommendation has not been acted on within two years to the NERC Planning and Operating Committees.	The Regional Reliability Organization has not reviewed the final report recommendations or did not notify the NERC Planning and Operating Committees.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-005-1	R1.	Each Transmission Operator shall have a restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system, including necessary operating instructions and procedures to cover emergency conditions, and the loss of vital telecommunications channels. Each Transmission Operator shall include the applicable elements listed in Attachment 1-EOP-005 in developing a restoration plan.	The responsible entity has a restoration plan that includes 75 % or more but less than 100% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 50% to 75% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 25% - 50% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes less than 25% of the applicable elements listed in Attachment 1 OR the responsible entity has no restoration plan.
EOP-005-1	R2.	Each Transmission Operator shall review and update its restoration plan at least annually and whenever it makes changes in the power system network, and shall correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review or update its restoration plan when it made changes in the power system network.	The Transmission Operator failed to review and update its restoration plan at least annually.	The Transmission Operator failed to review and update its restoration plan at least annually or whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review and update its restoration plan at least annually and whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.
EOP-005-1	R3.	Each Transmission Operator shall develop restoration plans with a priority of restoring the integrity of the Interconnection.	N/A	N/A	N/A	The Transmission Operator's restoration plans failed to make restoration of the integrity of the Interconnection a priority.
EOP-005-1	R4.	Each Transmission Operator shall coordinate its restoration plans with the Generator Owners and Balancing Authorities within its area, its Reliability Coordinator, and neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate its restoration plans with 5% or less of the entities identified in the requirement.	The Transmission Operator failed to coordinate its restoration plans with more than 5% up to (and including) 10% of the entities identified in the	The Transmission Operator failed to coordinate its restoration plans with more than 10% up to (and including) 15% of the entities identified in	The Transmission Operator failed to coordinate its restoration plans with more than 15% of the entities identified in the requirement.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requirement.	the requirement.	
EOP-005-1	R5.	Each Transmission Operator and Balancing Authority shall periodically test its telecommunication facilities needed to implement the restoration plan.	N/A	N/A	N/A	The responsible entity failed to periodically test its telecommunication facilities needed to implement the restoration plan.
EOP-005-1	R6.	Each Transmission Operator and Balancing Authority shall train its operating personnel in the implementation of the restoration plan. Such training shall include simulated exercises, if practicable.	The Transmission Operator or Balancing Authority failed to train 5% or less of its operating personnel in the implementation of the restoration plan.	The Transmission Operator or Balancing Authority failed to train more than 5% up to (and including) 10 % of its operating personnel in the implementation of the restoration plan.	The Transmission Operator or Balancing Authority failed to train more than 10 % up to (and including) 15% of its operating personnel in the implementation of the restoration plan.	The Transmission Operator or Balancing Authority failed to train more than 15% of its operating personnel in the implementation of the restoration plan.
EOP-005-1	R7.	Each Transmission Operator and Balancing Authority shall verify the restoration procedure by actual testing or by simulation.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority did not verify the restoration procedure by actual testing or by simulation.
EOP-005-1	R8.	Each Transmission Operator shall verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.	N/A	N/A	N/A	The Transmission Operator failed to verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requirements for the Transmission Operator's area.
EOP-005-1	R9.	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request. Such documentation may include Cranking Path diagrams.	N/A	N/A	The Transmission Operator documented the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started, but did not provide the documentation as requested by the Regional Reliability Organization.	The Transmission Operator failed to document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started.
EOP-005-1	R10.	The Transmission Operator shall demonstrate, through simulation or testing, that the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	For less than 25% of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.	For 25% or more, but less than 50% of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.	For 50% or more, but less than 75% of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.	For 75% or more of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.
EOP-005-1	R10.1.	The Transmission Operator shall perform this simulation or testing at least once every five years.	N/A	N/A	N/A	The Transmission Operator failed to perform the required simulation or testing at least once every five years.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-005-1	R11.	Following a disturbance in which one or more areas of the Bulk Electric System become isolated or blacked out, the affected Transmission Operators and Balancing Authorities shall begin immediately to return the Bulk Electric System to normal.	The responsible entity failed to comply with less than 25% of the number of sub-components.	The responsible entity failed to comply with 25% or more and less than 50% of the number of sub-components.	The responsible entity failed to comply with 50% or more and less than 75% of the number of sub-components.	The responsible entity failed to comply with more than 75% of the number of sub-components.
EOP-005-1	R11.1.	The affected Transmission Operators and Balancing Authorities shall work in conjunction with their Reliability Coordinator(s) to determine the extent and condition of the isolated area(s).	N/A	N/A	N/A	The responsible entity failed to work in conjunction with their Reliability Coordinator to determine the extent and condition of the isolated area(s)
EOP-005-1	R11.2.	The affected Transmission Operators and Balancing Authorities shall take the necessary actions to restore Bulk Electric System frequency to normal, including adjusting generation, placing additional generators on line, or load shedding.	N/A	N/A	N/A	The affected Transmission Operators and Balancing Authorities failed to take the necessary actions to restore Bulk Electric System frequency to normal.
EOP-005-1	R11.3.	The affected Balancing Authorities, working with their Reliability Coordinator(s), shall immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments as needed to facilitate the restoration. The affected Balancing Authorities shall make all attempts to maintain the adjusted Interchange Schedules, whether generation control is manual or automatic.	N/A	N/A	The responsible entity failed to make all attempts to maintain adjusted Interchange Schedules as required in R11.3	The responsible entity failed to immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments to facilitate the restoration as required

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						in R11.3.
EOP-005-1	R11.4.	The affected Transmission Operators shall give high priority to restoration of off-site power to nuclear stations.	N/A	N/A	N/A	The affected Transmission Operators failed to give high priority to restoration of off-site power to nuclear stations.
EOP-005-1	R11.5.	The affected Transmission Operators may resynchronize the isolated area(s) with the surrounding area(s) when the following conditions are met:	N/A	N/A	N/A	The Transmission Operator attempted to resynchronize an isolated area(s) with a surrounding area(s) when one (1) or more of the sub-requirements of R11.5 were not met.
EOP-005-1	R11.5.1.	Voltage, frequency, and phase angle permit.	N/A	N/A	N/A	N/A
EOP-005-1	R11.5.2.	The size of the area being reconnected and the capacity of the transmission lines effecting the reconnection and the number of synchronizing points across the system are considered.	N/A	N/A	N/A	N/A
EOP-005-1	R11.5.3.	Reliability Coordinator(s) and adjacent areas are notified and Reliability Coordinator approval is given.	N/A	N/A	N/A	N/A
EOP-005-1	R11.5.4.	Load is shed in neighboring areas, if required, to permit successful interconnected system restoration.	N/A	N/A	N/A	N/A
EOP-006-1	R1.	Each Reliability Coordinator shall be aware of the restoration plan of each Transmission Operator in its Reliability Coordinator Area in accordance with NERC and regional requirements.	The Reliability Coordinator is not aware of 5% or less of its Transmission Operators' restoration plans.	The Reliability Coordinator is not aware of more than 5% up to (and including) 10% of its Transmission Operators'	The Reliability Coordinator is not aware of more than 10% up to (and including) 15% of its Transmission Operators' restoration	The Reliability Coordinator is not aware of more than 15% of its Transmission Operators' restoration

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				restoration plans.	plans.	plans.
EOP-006-1	R2.	The Reliability Coordinator shall monitor restoration progress and coordinate any needed assistance.	N/A	N/A	The Reliability Coordinator failed to monitor restoration progress or failed to coordinate assistance.	The Reliability Coordinator failed to monitor restoration progress and failed to coordinate assistance.
EOP-006-1	R3.	The Reliability Coordinator shall have a Reliability Coordinator Area restoration plan that provides coordination between individual Transmission Operator restoration plans and that ensures reliability is maintained during system restoration events.	N/A	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not provide coordination between less than 10% of its individual Transmission Operator restoration plans.	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not provide coordination between 10% or more of the Transmission Operator restoration plans.	The Reliability Coordinator does not have a Reliability Coordinator Area restoration plan. OR The Reliability Coordinator's Reliability Coordinator Area restoration plan does not ensure reliability is maintained during system restoration events.
EOP-006-1	R4.	The Reliability Coordinator shall serve as the primary contact for disseminating information regarding restoration to neighboring Reliability Coordinators and Transmission Operators or Balancing Authorities not immediately involved in restoration.	N/A	N/A	N/A	The Reliability Coordinator failed to serve as primary contact for disseminating information regarding restoration in accordance with Requirement R4.
EOP-006-1	R5.	Reliability Coordinators shall approve, communicate, and coordinate the re-synchronizing of major system islands or synchronizing points so as not to cause a Burden on adjacent Transmission Operator, Balancing Authority, or Reliability	N/A	N/A	N/A	The Reliability Coordinator failed to approve, communicate, and coordinate the re-synchronizing of

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Coordinator Areas.				major system islands or synchronizing points as stated in Requirement R5.
EOP-006-1	R6.	The Reliability Coordinator shall take actions to restore normal operations once an operating emergency has been mitigated in accordance with its restoration plan.	N/A	N/A	N/A	The Reliability Coordinator failed to take actions to restore normal operations once an operating emergency was mitigated in accordance with its restoration plan.
EOP-008-0	R1.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have a plan to continue reliability operations in the event its control center becomes inoperable. The contingency plan must meet the following requirements:	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with one of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with two of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with three or four of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with more than four of the sub-requirements.
EOP-008-0	R1.1.	The contingency plan shall not rely on data or voice communication from the primary control facility to be viable.	The responsible entity's contingency plan relies on data or voice communication from the primary control facility for up to 25% of the functions identified in R1.2 and R1.3.	The responsible entity's contingency plan relies on data or voice communication from the primary control facility for 25% to 50% of the functions identified in R1.2 and R1.3.	The responsible entity's contingency plan relies on data or voice communication from the primary control facility for 50% to 75% of the functions identified in R1.2 and R1.3.	The responsible entity's contingency plan relies on data and voice communication from the primary control facility for more than 75% of the functions identified in R1.2 and R1.3.
EOP-008-0	R1.2.	The plan shall include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing basic tie line control and

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.
EOP-008-0	R1.3.	The contingency plan must address monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events. The plan shall list the critical facilities.	The responsible entity's contingency plan failed to address one of the elements listed in the requirement.	The responsible entity's contingency plan failed to address two of the elements listed in the requirement.	The responsible entity's contingency plan failed to address three of the elements listed in the requirement.	The responsible entity's contingency plan failed to address four or more of the elements listed in the requirement.
EOP-008-0	R1.4.	The plan shall include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.
EOP-008-0	R1.5.	The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.
EOP-008-0	R1.6.	The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing annual training to ensure that operating personnel

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						are able to implement the contingency plans.
EOP-008-0	R1.7.	The plan shall be reviewed and updated annually.	The responsible entity's plan was reviewed within 3 months of passing its annual review date.	The responsible entity's plan was reviewed within 6 months of passing its annual review date.	The responsible entity's plan was reviewed within 9 months of passing its annual review date.	The responsible entity's plan was reviewed more than 9 months of passing its annual review date.
EOP-008-0	R1.8.	Interim provisions must be included if it is expected to take more than one hour to implement the contingency plan for loss of primary control facility.	N/A	N/A	N/A	The responsible entity failed to make interim provisions when it is took more than one hour to implement the contingency plan for loss of primary control facility.
EOP-009-0	R1.	The Generator Operator of each blackstart generating unit shall test the startup and operation of each system blackstart generating unit identified in the BCP as required in the Regional BCP (Reliability Standard EOP-007-0_R1). Testing records shall include the dates of the tests, the duration of the tests, and an indication of whether the tests met Regional BCP requirements.	The Generator Operator Blackstart unit testing and recording is missing minor program/procedural elements.	Startup and testing of each Blackstart unit was performed, but the testing records are incomplete. The testing records are missing 25% or less of data requested in the requirement'.	The Generator Operator's failed to test 25% or less of the Blackstart units or testing records are incomplete. The testing records are missing between 25% and 50% of data requested in the requirement.	The Generator Operator failed to test more than 25% of its Blackstart units or does not have Blackstart testing records or is missing more than 50% of the required data.
EOP-009-0	R2.	The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.	N/A	N/A	N/A	The Generator Owner or Generator Operator did not provide the required blackstart documentation to its Regional Reliability Organization or upon request to NERC.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R1.	The Transmission Owner shall document, maintain, and publish facility connection requirements to ensure compliance with NERC Reliability Standards and applicable Regional Reliability Organization, subregional, Power Pool, and individual Transmission Owner planning criteria and facility connection requirements. The Transmission Owner's facility connection requirements shall address connection requirements for:	Not Applicable.	The Transmission Owner failed to do one of the following: Document or maintain or publish facility connection requirements as specified in the Requirement OR Failed to include one (1) of the components and specified in R1.1, R1.2 or R1.3.	The Transmission Owner failed to do one of the following: Document or maintain or publish its facility connection requirements as specified in the Requirement. OR Failed to include (2) of the components as specified in R1.1, R1.2 or R1.3 OR Failed to document or maintain or publish its facility connection requirements as specified in the Requirement **and** failed to include one (1) of the components as specified in R1.1, R1.2 or R1.3	The Transmission Owner did not develop facility connection requirements
FAC-001-0	R1.1.	Generation facilities,	N/A	N/A	N/A	N/A
FAC-001-0	R1.2.	Transmission facilities, and	N/A	N/A	N/A	N/A
FAC-001-0	R1.3.	End-user facilities	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R2.	The Transmission Owner's facility connection requirements shall address, but are not limited to, the following items:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.1.	Procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.2.	Procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R2.1.3.	Voltage level and MW and MVAR capacity or demand at point of connection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.4.	Breaker duty and surge protection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.5.	System protection and coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.6.	Metering and telecommunications.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.7.	Grounding and safety issues.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.8.	Insulation and insulation coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.9.	Voltage, Reactive Power, and power factor control.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.10.	Power quality impacts.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.11.	Equipment Ratings.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.12.	Synchronizing of facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.13.	Maintenance coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.14.	Operational issues (abnormal frequency and	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		voltages).				owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.15.	Inspection requirements for existing or new facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.16.	Communications and procedures during normal and emergency operating conditions.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R3.	The Transmission Owner shall maintain and update its facility connection requirements as required. The Transmission Owner shall make documentation of these requirements available to the users of the transmission system, the Regional Reliability Organization, and NERC on request (five business days).	The responsible entity made the requirements available more than five business days but less than or equal to 10 business days after a request.	The responsible entity made the requirements available more than 10 business days but less than or equal to 20 business days after a request.	The responsible entity made the requirements available more than 20 business days less than or equal to 30 business days after a request.	The responsible entity made the requirements available more than 30 business days after a request.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-002-1	R1.	The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:	The Responsible Entity failed to include in their assessment one of the subrequirements.	The Responsible Entity failed to include in their assessment two of the subrequirements.	The Responsible Entity failed to include in their assessment three of the subrequirements.	The Responsible Entity failed to include in their assessment four or more of the subrequirements.
FAC-002-1	R1.1.	Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evaluation.
FAC-002-1	R1.2.	Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity’s assessment did not include the ensurance of compliance.
FAC-002-1	R1.3.	Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity’s assessment did not include the evidence of coordination.
FAC-002-1	R1.4.	Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evidence of the studies.
FAC-002-1	R1.5.	Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		coordinated recommendations.				documentation.
FAC-002-1	R2. (Retired)	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).	The responsible entity provided the documentation more than 30 calendar days, but not more than 45 calendar days, after a request.	The responsible entity provided the documentation more than 45 calendar days, but not more than 60 calendar days, after a request.	The responsible entity provided the documentation more than 60 calendar days, but not more than 120 calendar days, after a request.	The responsible entity provided the documentation more than 120 calendar days after a request or was unable to provide the documentation.
FAC-003-1	R1.	The Transmission owner shall prepare, and keep current, a formal transmission vegetation management program (TVMP). The TVMP shall include the Transmission Owner's objectives, practices, approved procedures, and work Specifications. 1. ANSI A300, Tree Care Operations – Tree, Shrub, and Other Woody Plant Maintenance – Standard Practices, while not a requirement of this standard, is considered to be an industry best practice.	The responsible entity did not include and keep current one of the four required elements of its TVMP, as directed by the requirement.	The responsible entity did not include and keep current two of the four required elements of its TVMP, as directed by the requirement.	The responsible entity did not include and keep current three of the four required elements of its TVMP, as directed by the requirement.	The responsible entity did not include and keep current all required elements of the TVMP, as directed by the requirement.
FAC-003-1	R1.1.	The TVMP shall define a schedule for and the type (aerial, ground) of ROW vegetation inspections. This schedule should be flexible enough to adjust for changing conditions. The inspection schedule shall be based on the anticipated growth of vegetation and any other environmental or operational factors that could impact the relationship of vegetation to the Transmission Owner's transmission lines.	N/A	N/A	The applicable entity TVMP did not define a schedule, as directed by the requirement, or the type of ROW vegetation inspections, as directed by the requirement.	The applicable entity TVMP did not define a schedule, as directed by the requirement, nor the type of ROW vegetation inspections, as directed by the requirement.
FAC-003-1	R1.2.	The Transmission Owner, in the TVMP, shall identify and document clearances between vegetation and any overhead, ungrounded supply conductors, taking into	N/A	N/A	N/A	The responsible entity, in its TVMP, failed to identify and document clearances between

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		consideration transmission line voltage, the effects of ambient temperature on conductor sag under maximum design loading, and the effects of wind velocities on conductor sway. Specifically, the Transmission Owner shall establish clearances to be achieved at the time of vegetation management work identified herein as Clearance 1, and shall also establish and maintain a set of clearances identified herein as Clearance 2 to prevent flashover between vegetation and overhead ungrounded supply conductors.				vegetation and any overhead, ungrounded supply conductors. OR The responsible entity, in its TVMP, failed to take into consideration transmission line voltage, or the effects of ambient temperature on conductor sag under maximum design loading, or the effects of wind velocities on conductor sway. OR The responsible entity, in its TVMP, failed to establish Clearance 1 or Clearance 2 values.
FAC-003-1	R1.2.1.	Clearance 1 — The Transmission Owner shall determine and document appropriate clearance distances to be achieved at the time of transmission vegetation management work based upon local conditions and the expected time frame in which the Transmission Owner plans to return for future vegetation management work. Local conditions may include, but are not limited to: operating voltage, appropriate vegetation management techniques, fire risk, reasonably anticipated tree and conductor movement, species types and growth rates, species failure characteristics, local climate and rainfall patterns, line terrain and elevation, location	N/A	N/A	N/A	The responsible entity failed to determine and document an appropriate clearance distance to be achieved at the time of transmission vegetation management work taking into account local conditions and the expected time frame in which the responsible entity expects to return for future vegetation

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of the vegetation within the span, and worker approach distance requirements. Clearance 1 distances shall be greater than those defined by Clearance 2 below.				management work. OR The responsible entity documented a Clearance 1 value that was smaller than its Clearance 2 value.
FAC-003-1	R1.2.2.	Clearance 2 — The Transmission Owner shall determine and document specific radial clearances to be maintained between vegetation and conductors under all rated electrical operating conditions. These minimum clearance distances are necessary to prevent flashover between vegetation and conductors and will vary due to such factors as altitude and operating voltage. These Transmission Owner-specific minimum clearance distances shall be no less than those set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard 516-2003 (*Guide for Maintenance Methods on Energized Power Lines*) and as specified in its Section 4.2.2.3, Minimum Air Insulation Distances without Tools in the Air Gap.	N/A	N/A	N/A	The responsible entity failed to determine and document Clearance 2 values taking into account local conditions and the expected time frame in which the responsible entity expects to return for future vegetation management work.
FAC-003-1	R1.2.2.1.	Where transmission system transient overvoltage factors are not known, clearances shall be derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.	N/A	N/A	N/A	Where transmission system transient overvoltage factors were not known, clearances were not derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-003-1	R1.2.2.2.	Where transmission system transient overvoltage factors are known, clearances shall be derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.	Not Applicable.	Not Applicable.	Not Applicable.	Where transmission system transient overvoltage factors are known, clearances were not derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.
FAC-003-1	R1.3.	All personnel directly involved in the design and implementation of the TVMP shall hold appropriate qualifications and training, as defined by the Transmission Owner, to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, one of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, 5% or less of those persons did not hold appropriate qualifications and training to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, two of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, more than 5% up to (and including) 10%of those persons did not hold appropriate qualifications and training to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, three of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, more than 10% up to (and including) 15%of those persons did not hold appropriate qualifications and training to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, more than three of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, more than 15% of those persons did not hold appropriate qualifications and training to perform their duties.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-003-1	R1.4.	Each Transmission Owner shall develop mitigation measures to achieve sufficient clearances for the protection of the transmission facilities when it identifies locations on the ROW where the Transmission Owner is restricted from attaining the clearances specified in Requirement 1.2.1.	N/A	N/A	N/A	The responsible entity's TVMP does not include mitigation measures to achieve sufficient clearances where restrictions to the ROW are in effect.
FAC-003-1	R1.5.	Each Transmission Owner shall establish and document a process for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage. This is so that action (temporary reduction in line rating, switching line out of service, etc.) may be taken until the threat is relieved.	N/A	N/A	N/A	The responsible entity did not establish or did not document a process for the immediate communication of vegetation conditions that present an imminent threat of line outage, as directed by the requirement.
FAC-003-1	R2.	The Transmission Owner shall create and implement an annual plan for vegetation management work to ensure the reliability of the system. The plan shall describe the methods used, such as manual clearing, mechanical clearing, herbicide treatment, or other actions. The plan should be flexible enough to adjust to changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors that may have an impact on the reliability of the transmission systems. Adjustments to the plan shall be documented as they occur. The plan should take into consideration the time required to obtain permissions or permits from landowners or regulatory authorities. Each Transmission Owner shall have systems and procedures for documenting and tracking	The responsible entity did not meet one of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the	The responsible entity did not meet two of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan)	The responsible entity did not meet the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	The responsible entity does not have an annual plan for vegetation management. OR The responsible entity has not implemented the annual plan for vegetation management.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the planned vegetation management work and ensuring that the vegetation management work was completed according to work specifications.	requirement.	specified in the requirement.		
FAC-003-1	R3.	The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.	The responsible entity failed to provide a quarterly outage report, but did not experience any reportable outages. OR The responsible entity provided a quarterly report, but failed to report in the manner specified by one or more of the following subcomponents of R3: R3.1 or R3.2.	The responsible entity provided a quarterly report, but failed to include information required by R3.3.	The responsible entity provided a quarterly outage report, but failed to include a reportable Category 3 outage as described in R3.4.3.	The responsible entity experienced reportable outages but failed to provide a quarterly report. OR The responsible entity provided a quarterly outage report, but failed to include a reportable Category 1 (as described in R3.4.1) or Category 2 outage (as described in R3.4.2).
FAC-003-1	R3.1.	Multiple sustained outages on an individual line, if caused by the same vegetation, shall be reported as one outage regardless of the actual number of outages within a 24-hour period.	N/A	N/A	N/A	N/A
FAC-003-1	R3.2.	The Transmission Owner is not required to report to the RRO, or the RRO's designee, certain sustained transmission line outages caused by vegetation: (1) Vegetation-related outages that result from vegetation falling into lines from outside the ROW that result from natural disasters shall not be considered reportable (examples of disasters that could create non-reportable outages include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, major storms as defined either by the Transmission Owner or an applicable	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		regulatory body, ice storms, and floods), and (2) Vegetation-related outages due to human or animal activity shall not be considered reportable (examples of human or animal activity that could cause a non-reportable outage include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural activities or horticultural or agricultural activities, or removal or digging of vegetation).				
FAC-003-1	R3.3.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, shall include at a minimum: the name of the circuit(s) outaged, the date, time and duration of the outage; a description of the cause of the outage; other pertinent comments; and any countermeasures taken by the Transmission Owner.	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.	An outage shall be categorized as one of the following:	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.1.	Category 1 — Grow-ins: Outages caused by vegetation growing into lines from vegetation inside and/or outside of the ROW;	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.2.	Category 2 — Fall-ins: Outages caused by vegetation falling into lines from inside the ROW;	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.3.	Category 3 — Fall-ins: Outages caused by vegetation falling into lines from outside the ROW.	N/A	N/A	N/A	N/A
FAC-003-1	R4.	The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions	Not applicable.	Not applicable.	The RRO did not submit a quarterly report to NERC for a	The RRO did not submit a quarterly report to NERC for more than two

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		taken by the RRO as a result of any of the reported outages.			single quarter.	consecutive quarters.
FAC-008-1	R1.	The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:	The responsible entity failed to include in their methodology one of the subcomponents of R1.3, (R1.3.1 to R1.3.5).	The responsible entity failed to include in their methodology two of the subcomponents of R1.3, (R1.3.1 to R1.3.5).	The responsible entity rating methodology did not address either of the sub-components of R1.2 (R1.2.1 or R1.2.2). OR The responsible entity failed to include in their methodology three of the subcomponents of R1.3, (R1.3.1 to R1.3.5).	The Transmission Owner or Generation Owner does not have a documented Facility Ratings Methodology for use in developing facility ratings. The responsible entity's rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in R1.1. OR The responsible entity rating methodology did not address the components of R1.2, (R1.2.1 and R1.2.2). OR The responsible entity failed to include in their methodology four or more of the subcomponents of R1.3, (R1.3.1 to R1.3.5).
FAC-008-1	R1.1.	A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.	N/A	N/A	N/A	N/A
FAC-008-1	R1.2.	The method by which the Rating (of major BES equipment that comprises a Facility) is	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		determined.				
FAC-008-1	R1.2.1.	The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.	N/A	N/A	N/A	N/A
FAC-008-1	R1.2.2.	The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.	Consideration of the following:	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.1.	Ratings provided by equipment manufacturers.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.2.	Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.3.	Ambient conditions.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.4.	Operating limitations.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.5.	Other assumptions.	N/A	N/A	N/A	N/A
FAC-008-1	R2. (Retired)	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.	The responsible entity made the Facility Ratings Methodology available within more than 15 business days but less than or equal to 25 business days after a request.	The responsible entity made the Facility Ratings Methodology available within more than 25 business days but less than or equal to 35 business days after a request.	The responsible entity made the Facility Ratings Methodology available within more than 35 business days but less than or equal to 45 business days after a request.	The responsible entity failed to make available the Facility Ratings Methodology available in more than 45 business days after a request.
FAC-008-1	R3. (Retired)	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a	The responsible entity provided a response in more than 45 calendar days but less than or	The responsible entity provided a response in more than 60 calendar	The responsible entity provided a response in more than 70 calendar days but less than or	The responsible entity failed to provide a response as required in more than 80 calendar

Formatted: Font color: Red

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.	equal to 60 calendar days after a request.	days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings Methodology but did not indicate why no change will be made.	equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings Methodology.	days after a request.
FAC-008-3	R1.	Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. [See standard for documentation requirements]	N/A	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
FAC-008-3	R2.	Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. [See standard for methodology	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1.	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		requirements]	• 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	• 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
FAC-008-3	R3.	Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: [See standard for methodology requirements]	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2 OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3:

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					• 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	• 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
FAC-008-3	R4. (Retired)	Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.	The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.	The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)
FAC-008-3	R5. (Retired)	If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.	The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)	The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility	The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation.	The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)

Formatted: Font color: Red

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)	(R5)	
FAC-008-3	R6.	Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
FAC-008-3	R7.	Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requesting entities.
FAC-008-3	R8.	Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): [See standard for requirements of providing requested information]	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			requesting entity. (R8, Part 8.2)	entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	required Rating information to the requesting entity. (R8, Part 8.2)	Rating information to the requesting entity. (R8, Part 8.1)
FAC-009-1	R1.	The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for 5% or less of its solely owned and jointly owned Facilities.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for more than 5% up to (and including) 10% of its solely owned and jointly owned Facilities.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for more than 15% of its solely owned and jointly owned Facilities.
FAC-009-1	R2.	The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to 15 calendar days.	The Transmission Owner or Generator Owner provided its Facility Ratings to all but one of the requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to two of the requesting entities.	The Transmission Owner or Generator Owner has provided its Facility Ratings to none of the requesting entities within 30 calendar days of the associated schedules.
FAC-010-2.1	R1	The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				address R1.2		OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
FAC-010-2.1	R2.	The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 – R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
FAC-010-2.1	R3.	The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			through R3.6.	through R3.6.		R3.1 through R3.6.
FAC-010-2.1	R4.	The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:	One or both of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	One of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of	One of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and	One of the following: The Planning Authority failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				the change.	changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
FAC-010-2.1	R5. (Retired)	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority	The Planning Authority received documented technical	The Planning Authority received documented	The Planning Authority received documented technical comments on	The Planning Authority received documented technical

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.
FAC-011-2	R1.	The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
FAC-011-2	R2.	The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance	The Reliability Coordinator's SOL Methodology	Not applicable.	The Reliability Coordinator's SOL Methodology	The Reliability Coordinator's SOL Methodology

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		consistent with the following:	requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)		requires that SOLs are set to meet BES performance in the precontingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
FAC-011-2	R3.	The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
FAC-011-2	R4	The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:	One or both of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed	One of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days after the effectiveness of the change.	methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						methodology was provided up to 30 calendar days after the effectiveness of the change.
FAC-011-2	R5. (Retired)	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.
FAC-013-1	R1.	The Reliability Coordinator and Planning Authority shall each establish a set of inter-regional and intra-regional Transfer Capabilities that is consistent with its current Transfer Capability Methodology.	The responsible entity has established a set of Transfer Capabilities, but 5% or less of all Transfer Capabilities required to be established, are inconsistent with the current Transfer Capability	The responsible entity has established a set of Transfer Capabilities, but more than 5% up to (and including) 10% of all Transfer Capabilities required to be established,	The responsible entity has established a set of Transfer Capabilities, but more than 10% up to (and including) 15% of all Transfer Capabilities required to be established, are inconsistent with the current Transfer	The responsible entity has established a set of Transfer Capabilities, but more than 15% of those Transfer Capabilities are not consistent with the current Transfer Capability Methodology

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Methodology.	are inconsistent with the current Transfer Capability Methodology.	Capability Methodology.	OR The responsible entity has not established a set of Transfer Capabilities.
FAC-013-1	R2.	The Reliability Coordinator and Planning Authority shall each provide its inter-regional and intra-regional Transfer Capabilities to those entities that have a reliability-related need for such Transfer Capabilities and make a written request that includes a schedule for delivery of such Transfer Capabilities as follows:	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting one schedule by up to 15 calendar days.	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting two schedules.	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting more than two schedules.	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting all schedules within 30 calendar days of the associated schedules.
FAC-013-1	R2.1.	The Reliability Coordinator shall provide its Transfer Capabilities to its associated Regional Reliability Organization(s), to its adjacent Reliability Coordinators, and to the Transmission Operators, Transmission Service Providers and Planning Authorities that work in its Reliability Coordinator Area.	The responsible entity failed to provide Transfer Capabilities to 5% or less of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 5% up to (and including) 10% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 10% up to (and including) 15% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 15% of the required entities.
FAC-013-1	R2.2.	The Planning Authority shall provide its Transfer Capabilities to its associated Reliability Coordinator(s) and Regional Reliability Organization(s), and to the Transmission Planners and Transmission Service Provider(s) that work in its Planning Authority Area.	The responsible entity failed to provide Transfer Capabilities 5% or less of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 5% up to (and including) 10% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 10% up to (and including) 15% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 15% of the required entities.
FAC-013-2	R1.	Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology:	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		information: [See standard pdf for requirements of the Transfer Capability methodology]		into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	• Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.
FAC-013-2	R2.	Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: [See standard pdf for requirements of issuing the Transfer Capability Methodology]	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	90 calendar days but not more than 120 calendar days after receipt of a request.	methodology more than 120 calendar days after receipt of a request.
FAC-013-2	R3. (Retired)	If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.
FAC-013-2	R4.	During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days,	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planning Horizon.	calendar days.	more than 30 calendar days, but not by more than 60 calendar days.	but not by more than 90 calendar days.	calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.
FAC-013-2	R5.	Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
FAC-013-2	R6.	If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days	The Planning Coordinator provided the requested data as required in Requirement R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information.	after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.
FAC-014-2	R1.	The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.	There are SOLs, for the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs for the Reliability Coordinator Area, but 75% or more of these the SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)
FAC-014-2	R2.	The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 75% or more of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)
FAC-014-2	R3.	The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology.	There are SOLs, for the Planning Coordinator Area, but from 1% up to, but less than, 25% of these	There are SOLs, for the Planning Coordinator Area, but 25% or more, but less than 50% of	There are SOLs for the Planning Coordinator Area, but 50% or more, but less than 75% of these SOLs are	There are SOLs, for the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	inconsistent with the Planning Coordinator's SOL Methodology. (R3)	with the Planning Coordinator's SOL Methodology. (R3)
FAC-014-2	R4.	The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology.	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but up to 25% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)
FAC-014-2	R5.	The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows:	The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all the requesting entities but missed meeting one or more of the schedules by less than 15 calendar days. (R5)	One of the following: The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all but one of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the	One of the following: The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all but two of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 30	One of the following: The responsible entity failed to provide its SOLs (including the subset of SOLs that are IROLs) to more than two of the requesting entities within 45 calendar days of the associated schedules. (R5) OR The supporting information provided with the IROLs does not address 5.1.1 and 5.1.2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				schedules for 15 or more but less than 30 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.4	or more but less than 45 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.3	
FAC-014-2	R6.	The Planning Authority shall identify the subset of multiple contingencies (if any), from Reliability Standard TPL-003 which result in stability limits.	The Planning Authority failed to notify the Reliability Coordinator in accordance with R6.2	Not applicable.	The Planning Authority identified the subset of multiple contingencies which result in stability limits **but** did not provide the list of multiple contingencies and associated limits to one Reliability Coordinator that monitors the Facilities associated with these limits. (R6.1)	The Planning Authority did not identify the subset of multiple contingencies which result in stability limits. (R6) OR The Planning Authority identified the subset of multiple contingencies which result in stability limits **but** did not provide the list of multiple contingencies and associated limits to more than one Reliability Coordinator that monitors the Facilities associated with these limits. (R6.1)
FAC-501-WECC-1	R1.	Transmission Owners shall have a TMIP detailing their inspection and maintenance	The TMIP does not include associated	The TMIP does not include associated	The TMIP does not include associated	The TMIP does not include associated

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		requirements that apply to all transmission facilities necessary for System Operating Limits associated with each of the transmission paths identified in table titled "Major WECC Transfer Paths in the Bulk Electric System."	Facilities for one of the Paths identified in Attachment 1 FAC-501-WECC-1 as required by R.1 but Transmission Owners are performing maintenance and inspection for the missing Facilities.	Facilities for two of the Paths identified in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" as required by R.1 and Transmission Owners are not performing maintenance and inspection for the missing Facilities.	Facilities for three of the Paths identified in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" as required by R.1 and Transmission Owners are not performing maintenance and inspection for the missing Facilities.	Facilities for more than three of the Paths identified in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" as required by R.1 and Transmission Owners are not performing maintenance and inspection for the missing Facilities.
FAC-501-WECC-1	R1.1.	Transmission Owners shall annually review their TMIP and update as required.	Transmission Owners did not review their TMIP annually as required by R.1.1.	N/A	N/A	N/A
FAC-501-WECC-1	R2.	Transmission Owners shall include the maintenance categories in Attachment 1-FAC-501-WECC-1 when developing their TMIP.	The TMIP does not include one maintenance category identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.	The TMIP does not include two maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.	The TMIP does not include three maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.	The TMIP does not exist or does not include more than three maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.
FAC-501-WECC-1	R3.	Transmission Owners shall implement and follow their TMIP.	Transmission Owners do not have maintenance and inspection records as	Transmission Owners are not performing maintenance and	Transmission Owners are not performing maintenance and inspection for two	Transmission Owners are not performing maintenance and inspection for more

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by R.3 but have evidence that they are implementing and following their TMIP.	inspection for one maintenance category identified in Attachment 1 FAC-501-WECC-1 as required in R3.	maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required in R3.	than two maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required in R3.

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-001-3	R1.	The Load-Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for:	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)
INT-001-3	R1.1.	All Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.
INT-001-3	R2.	The Sink Balancing Authority shall ensure that Arranged Interchange is submitted to the Interchange Authority:	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-001-3	R2.1.	If a Purchasing-Selling Entity is not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.
INT-001-3	R2.2.	For each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.
INT-003-3	R1.	Each Receiving Balancing Authority shall confirm Interchange Schedules with the Sending Balancing Authority prior to implementation in the Balancing Authority's ACE equation.	There shall be a separate Lower VSL, if either of the following conditions exists: One instance of entering a schedule into its ACE equation without confirming the	There shall be a separate Moderate VSL, if either of the following conditions exists: Two instances of entering a schedule into its ACE equation	There shall be a separate High VSL, if either of the following conditions exists: Three instances of entering a schedule into its ACE equation without confirming the schedule	There shall be a separate Severe VSL, if either of the following conditions exists: Four or more instances of entering a schedule into its ACE equation without

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. One instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Two instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	as specified in R1, R1.1, R1.1.1 and R1.1.2. Three instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Four or more instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-003-3	R1.1.	The Sending Balancing Authority and Receiving Balancing Authority shall agree on Interchange as received from the Interchange Authority, including:	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-3	R1.1.1.	Interchange Schedule start and end time.	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-3	R1.1.2	Energy profile.	The Balancing Authority experienced	The Balancing Authority	The Balancing Authority experienced	The Balancing Authority experienced

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-3	R1.2.	If a high voltage direct current (HVDC) tie is on the Scheduling Path, then the Sending Balancing Authorities and Receiving Balancing Authorities shall coordinate the Interchange Schedule with the Transmission Operator of the HVDC tie.	The sending or receiving Balancing Authority experienced one instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced two instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced three instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced four instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-004-2	R1.	At such time as the reliability event allows for the reloading of the transaction, the entity that initiated the curtailment shall release the limit on the Interchange Transaction tag to allow reloading the transaction and shall communicate the release of the limit to the Sink Balancing Authority.	The entity that initiated the curtailment failed to communicate the transaction reload to the Sink Balancing Authority	The entity that initiated the curtailment failed to reload the transaction and failed to communicate to the Sink Balancing Authority	N/A	N/A
INT-004-2	R2.	The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:	N/A	N/A	The responsible entity failed to update the tag when required by sub-requirements R2.1 or R2.2.	The responsible entity failed to update the tag when required by sub-requirement R2.3.
INT-004-2	R2.1.	The average energy profile in an hour is greater than 250 MW and in that hour the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +10%.				
INT-004-2	R2.2.	The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +25 megawatt-hours.	N/A	N/A	N/A	N/A
INT-004-2	R2.3.	A Reliability Coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons.	N/A	N/A	N/A	N/A
INT-005-3	R1.	Prior to the expiration of the time period defined in the timing requirements tables in this standard, Column A, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment to all reliability entities involved in the Interchange.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities
INT-005-3	R1.1.	When a Balancing Authority or Reliability Coordinator initiates a Curtailment to Confirmed or Implemented Interchange for reliability, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment only to the Source Balancing Authority and the Sink Balancing Authority.	N/A	N/A	The Responsible Entity initiated a Curtailment to Confirmed or Implemented Interchange for reliability but the Interchange Authority failed to distribute the Arranged Interchange information to the Source Balancing Authority or the Sink Balancing Authority.	The Responsible Entity initiated a Curtailment to Confirmed or Implemented Interchange for reliability but the Interchange Authority failed to distribute the Arranged Interchange information to the Source Balancing Authority and the Sink Balancing Authority.
INT-006-3	R1.	Prior to the expiration of the reliability	The Responsible	The Responsible	The Responsible Entity	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		assessment period defined in the timing requirements tables in this standard, Column B, the Balancing Authority and Transmission Service Provider shall respond to each On-time Request for Interchange (RFI), and to each Emergency RFI and Reliability Adjustment RFI from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange	Entity failed on one occasion to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	Entity failed on two occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	failed on three occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	Entity failed on four occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.
INT-006-3	R1.1.	Each involved Balancing Authority shall evaluate the Arranged Interchange with respect to:	The Balancing Authority failed to evaluate arranged interchange with respect to one of the requirements in the 3 sub-components.	N/A	The Balancing Authority failed to evaluate arranged interchange with respect to two of the requirements in the 3 sub-components.	The Balancing Authority failed to evaluate arranged interchange with respect to three of the requirements in the 3 sub-components.
INT-006-3	R1.1.1.	Energy profile (ability to support the magnitude of the Interchange).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Energy profile (ability to support the magnitude of the Interchange).
INT-006-3	R1.1.2.	Ramp (ability of generation maneuverability to accommodate).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Ramp (ability of generation maneuverability to accommodate).
INT-006-3	R1.1.3.	Scheduling path (proper connectivity of Adjacent Balancing Authorities).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Scheduling path (proper connectivity of Adjacent Balancing Authorities).

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-006-3	R1.2.	Each involved Transmission Service Provider shall confirm that the transmission service arrangements associated with the Arranged Interchange have adjacent Transmission Service Provider connectivity, are valid and prevailing transmission system limits will not be violated	The Transmission Service Provider experienced one instance of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced two instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced three instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experience four instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.
INT-007-1	R1.	The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:	The Interchange Authority failed to verify one time, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)	The Interchange Authority failed to verify two times, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)	The Interchange Authority failed to verify three times, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)	The Interchange Authority failed to verify four times, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)
INT-007-1	R1.1.	Source Balancing Authority megawatts equal sink Balancing Authority megawatts	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to

Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(adjusted for losses, if appropriate).	verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.2. (Retired)	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.	The following are defined:	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.1.	Generation source and load sink.	The Interchange Authority failed to verify one time, as	The Interchange Authority failed to verify two times, as	The Interchange Authority failed to verify three times, as	The Interchange Authority failed to verify four times, as

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.2.	Megawatt profile.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.3.	Ramp start and stop times.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.4.	Interchange duration.	The Interchange Authority failed to verify one time, as indicated in R1 that	The Interchange Authority failed to verify two times, as indicated in R1 that	The Interchange Authority failed to verify three times, as indicated in R1 that	The Interchange Authority failed to verify four times, as indicated in R1 that

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.4.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with minor exception and is substantially compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with some exception and is mostly compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval but was substantially deficient in meeting the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment did not provided approval and failed to meet the requirement.
INT-008-3	R1.	Prior to the expiration of the time period defined in the Timing Table, Column C, the Interchange Authority shall distribute to all Balancing Authorities (including Balancing Authorities on both sides of a direct current tie), Transmission Service Providers and Purchasing-Selling Entities involved in the Arranged Interchange whether or not the Arranged Interchange has transitioned to a Confirmed Interchange.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as deliniated in R1.1, R1.1.1 or R1.1.2.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities or no evidence provided.
INT-008-3	R1.1.	For Confirmed Interchange, the Interchange	The Interchange	The Interchange	The Interchange	The Interchange

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authority shall also communicate:	Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-3	R1.1.1.	Start and stop times, ramps, and megawatt profile to Balancing Authorities.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-3	R1.1.2.	Necessary Interchange information to NERC-identified reliability analysis services.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-009-1	R1.	The Balancing Authority shall implement Confirmed Interchange as received from the Interchange Authority.	N/A	N/A	N/A	The responsible entity failed to implement a Confirmed Interchange as received from the Interchange Authority.
INT-010-1	R1.	The Balancing Authority that experiences a loss of resources covered by an energy sharing agreement shall ensure that a request for an Arranged Interchange is submitted with a start time no more than 60 minutes	The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an	The responsible entity that experienced a loss of resources that exceeded 60	The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an	The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		beyond the resource loss. If the use of the energy sharing agreement does not exceed 60 minutes from the time of the resource loss, no request for Arranged Interchange is required.	energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was more than 60 minutes but less than 75 minutes beyond the resource loss.	minutes and was covered by an energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was 75 minutes or more, but less than 90 minutes beyond the resource loss.	energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was 90 minutes or more, but less than 105 minutes beyond the resource loss.	energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was more than 105 minutes beyond the resource loss. OR The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an energy sharing agreement, failed to ensure that a request for an Arranged Interchange was submitted.
INT-010-1	R2.	For a modification to an existing Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit the modified Arranged Interchange reflecting that modification within 60 minutes of the initiation of the event.	N/A	N/A	N/A	The responsible entity failed to direct a Balancing Authority to submit the modified Arranged Interchange reflecting the modification, within 60 minutes of the initiation of the event.
INT-010-1	R3.	For a new Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit an Arranged Interchange reflecting that Interchange schedule within 60 minutes of	N/A	N/A	N/A	The responsible entity failed to direct a Balancing Authority to submit an Arranged Interchange reflecting the new Interchange schedule within 60

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the initiation of the event.				minutes of the initiation of the event.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-001-1.1	R1.	Each Regional Reliability Organization, subregion, or interregional coordinating group shall establish one or more Reliability Coordinators to continuously assess transmission reliability and coordinate emergency operations among the operating entities within the region and across the regional boundaries.	The RRO, subregion or interregional coordinating group did not communicate the assignment of the Reliability Coordinators to operating entities clearly.	The RRO, subregion or interregional coordinating group did not clearly identify the coordination of Reliability Coordinator areas within the region.	The RRO, subregion or interregional coordinating group did not coordinate assignment of the Reliability Coordinators across regional boundaries.	The RRO, subregion or interregional coordinating group did not assign any Reliability Coordinators.
IRO-001-1.1	R2.	The Reliability Coordinator shall comply with a regional reliability plan approved by the NERC Operating Committee.	The Reliability Coordinator has failed to follow the administrative portions of its regional reliability plan.	The Reliability Coordinator has failed to follow steps in its regional reliability plan that requires operator interventions or actions.	The Reliability Coordinator does not have a regional reliability plan approved by the NERC OC.	The Reliability Coordinator does not have an unapproved regional reliability plan.
IRO-001-1.1	R3.	The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes.	N/A	N/A	The Reliability Coordinator cannot demonstrate that it has clear authority to act or direct actions to preserve transmission security and reliability of the Bulk Electric System.	The Reliability Coordinator failed to take or direct to preserve the reliability and security of the Bulk Electric System within 30 minutes of identifying those actions.
IRO-001-1.1	R4.	Reliability Coordinators that delegate tasks to other entities shall have formal operating agreements with each entity to which tasks are delegated. The Reliability Coordinator shall verify that all delegated tasks are understood, communicated, and addressed within its Reliability Coordinator Area. All	1. Less than 25% of the tasks are not documented in the agreement or 2. Less than 25% of the tasks are not performed according	1. More than 25% but 50% or less of the tasks are not documented in the agreement or 2. More than 25% but 50% or less of	1. More than 50% but 75% or less of the tasks are not documented in the agreement or 2. More than 50% but 75% or less of the tasks are not performed	1. There is no formal operating agreement for tasks delegated by the Reliability Coordinator, 2. More than 75% of the tasks are not

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		responsibilities for complying with NERC and regional standards applicable to Reliability Coordinators shall remain with the Reliability Coordinator.	to the agreement.	the tasks are not performed according to the agreement.	according to the agreement.	documented in the agreement or 3. More than 75% of the tasks are not performed according to the agreement.
IRO-001-1.1	R5.	The Reliability Coordinator shall list within its reliability plan all entities to which the Reliability Coordinator has delegated required tasks.	5% or less of the delegate entities are not identified in the reliability plan.	More than 5% up to (and including) 10% of the delegate entities are not identified in the reliability plan.	More than 10% up to (and including) 15% of the delegate entities are not identified in the reliability plan.	There is no reliability plan. OR More than 15% of the delegate entities are not identified in the reliability plan.
IRO-001-1.1	R6.	The Reliability Coordinator shall verify that all delegated tasks are carried out by NERC-certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that 5% or less of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that more than 5% up to (and including) 10% of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that more than 10% up to (and including) 15% of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that more than 15% of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.
IRO-001-1.1	R7.	The Reliability Coordinator shall have clear, comprehensive coordination agreements with adjacent Reliability Coordinators to ensure that System Operating Limit or Interconnection Reliability Operating Limit violation mitigation requiring actions in adjacent Reliability Coordinator Areas are coordinated.	The Reliability Coordinator has demonstrated the existence of coordination agreements with adjacent Reliability Coordinators but the agreements are not clear or comprehensive.	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to mitigate SOL and	The Reliability Coordinator has failed to demonstrate the existence of any coordination agreements with adjacent Reliability Coordinators.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigate SOL or IROL violations in its own Reliability Coordinator area.	IROL violations in its own Reliability Coordinator area.	
IRO-001-1.1	R8.	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.	N/A	The responsible entity could not comply with a directive due to qualified reasons (violation of safety, equipment or regulatory or statutory requirements) and did not immediately inform the Reliability Coordinator.	N/A	The responsible entity did not follow the Reliability Coordinator's directive.
IRO-001-1.1	R9.	The Reliability Coordinator shall act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of any other entity.	N/A	N/A	N/A	The Reliability Coordinator did not act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of one or more other entities.
IRO-003-2	R1.	Each Reliability Coordinator shall monitor all Bulk Electric System facilities, which may include sub-transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time,	N/A	N/A	The Reliability Coordinator failed to monitor **all** Bulk Electric System facilities, which may include sub-	The Reliability Coordinator failed to monitor Bulk Electric System facilities, which may include sub-transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.			transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.	information, within adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.
IRO-003-2	R2.	Each Reliability Coordinator shall know the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation. Reliability Coordinators shall also know the status of any facilities that may be required to assist area restoration objectives.	N/A	N/A	The Reliability Coordinator failed to know either the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation or the status of any facilities that may be required to assist area restoration objectives.	The Reliability Coordinator failed to know the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation and the status of any facilities that may be required to assist area restoration objectives.
IRO-006-5	R1.	Each Reliability Coordinator and Balancing Authority that receives a request pursuant to an Interconnection-wide transmission loading relief procedure (such as Eastern Interconnection TLR, WECC Unscheduled Flow Mitigation, or congestion management procedures from the ERCOT Protocols) from	N/A	N/A	N/A	The responsible entity received a request to curtail an Interchange Transaction crossing an Interconnection boundary pursuant to an Interconnection-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		any Reliability Coordinator, Balancing Authority, or Transmission Operator in another Interconnection to curtail an Interchange Transaction that crosses an Interconnection boundary shall comply with the request, unless it provides a reliability reason to the requestor why it cannot comply with the request.				wide transmission loading relief procedure from a Reliability Coordinator, Balancing Authority, or Transmission Operator, but the entity neither complied with the request, nor provided a reliability reason why it could not comply with the request.
IRO-006-EAST-1	R1.	When acting or instructing others to act to mitigate the magnitude and duration of the instance of exceeding an IROL within that IROL's TV, each Reliability Coordinator shall initiate, prior to or concurrently with the initiation of the Eastern Interconnection TLR procedure (or continuing management of this procedure if already initiated), one or more of the following actions: • Inter-area redispatch of generation • Intra-area redispatch of generation • Reconfiguration of the transmission system • Voluntary load reductions (e.g., Demand-side Management) • Controlled load reductions (e.g., load shedding)	N/A	N/A	N/A	When acting or instructing others to act to mitigate the magnitude and duration of the instance of exceeding an IROL within that IROL's Tv, the Reliability Coordinator did not initiate one or more of the actions listed under R1 prior to or in conjunction with the initiation of the Eastern Interconnection TLR procedure (or continuing management of this procedure if already initiated).
IRO-006-EAST-1	R2.	To ensure operating entities are provided with information needed to maintain an	The Reliability Coordinator initiating	The Reliability Coordinator	The Reliability Coordinator initiating	The Reliability Coordinator initiating

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		awareness of changes to the Transmission System, when initiating the Eastern Interconnection TLR procedure to prevent or mitigate an SOL or IROL exceedance, and at least every clock hour (with the exception of TLR-1, where an hourly update is not required) after initiation up to and including the hour when the TLR level has been identified as TLR Level 0, the Reliability Coordinator shall identify: 2.1. A list of congestion management actions to be implemented, and 2.2. One of the following TLR levels: TLR-1, TLR-2, TLR-3A, TLR-3B, TLR-4, TLR-5A, TLR-5B, TLR-6, TLR-0	the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for one clock hour during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.	initiating the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for two clock hours during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.	the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for three clock hours during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.	the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for four or more clock hours during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.
IRO-006-EAST-1	R3.	Upon the identification of the TLR level and a list of congestion management actions to be implemented, the Reliability Coordinator initiating this TLR procedure shall: o Notify all Reliability Coordinators in the Eastern Interconnection of the identified TLR level o Communicate the list of congestion management actions to be implemented to 1.) all Reliability Coordinators in the Eastern Interconnection, and 2.) those Reliability Coordinators in other Interconnections responsible for curtailing Interchange Transactions crossing Interconnection boundaries identified in the list of congestion management actions. o Request that the congestion management actions identified in Requirement R2, Part 2.1 be	The initiating Reliability Coordinator did not notify one or more Reliability Coordinators in the Eastern Interconnection of the TLR Level (3.1).	N/A	The initiating Reliability Coordinator did not communicate the list of congestion management actions to one or more of the Reliability Coordinators listed in Requirement R3, Part 3.2. OR The initiating Reliability Coordinator requested some, but not all, of the Reliability Coordinators identified in Requirement R3, Part 3.3 to implement the identified	The initiating Reliability Coordinator requested none of the Reliability Coordinators identified in Requirement R3, Part 3.3 to implement the identified congestion management actions.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implemented by: 1.) Each Reliability Coordinator associated with a Sink Balancing Authority for which Interchange Transactions are to be curtailed, 2.) Each Reliability Coordinator associated with a Balancing Authority in the Eastern Interconnection for which Network Integration Transmission Service or Native Load is to be curtailed, and 3.) Each Reliability Coordinator associated with a Balancing Authority in the Eastern Interconnection for which its Market Flow is to be curtailed.			congestion management actions.	
IRO-006-EAST-1	R4.	Each Reliability Coordinator that receives a request as described in Requirement R3, Part 3.3. shall, within 15 minutes of receiving the request, implement the congestion management actions requested by the issuing Reliability Coordinator as follows: • Instruct its Balancing Authorities to implement the Interchange Transaction schedule change requests. • Instruct its Balancing Authorities to implement the Network Integration Transmission Service and Native Load schedule changes for which the Balancing Authorities are responsible. • Instruct its Balancing Authorities to implement the Market Flow schedule changes for which the Balancing Authorities are responsible. • If an assessment determines shows that	N/A	N/A	N/A	The responding Reliability Coordinator did not, within 15 minutes of receiving a request, either 1.) implement all the requested congestion management actions, or 2.) implement none or some of the requested congestion management actions and replace the remainder with alternate congestion management actions, provided that: assessment showed that the actions replaced would have

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		one or more of the congestion management actions communicated in Requirement R3, Part 3.3 will result in a reliability concern or will be ineffective, the Reliability Coordinator may replace those specific actions with alternate congestion management actions, provided that: o The alternate congestion management actions have been agreed to by the initiating Reliability Coordinator, and o The assessment shows that the alternate congestion management actions will not adversely affect reliability.				resulted in a reliability concern or would have been ineffective, the alternate congestion management actions were agreed to by the initiating Reliability Coordinator, and assessment determined that the alternate congestion management actions would not adversely affect reliability.
IRO-006-TRE-1	R1.	The RC shall have procedures to identify and mitigate exceedances of identified Interconnection Reliability Operating Limits (IROL) and System Operating Limits (SOL) that will not be resolved by the automatic actions of the ERCOT Nodal market operations system. The procedures shall address, but not be limited to, one or more of the following: redispatch of generation; reconfiguration of the Transmission system; controlled load reductions (including both firm and non-firm load shedding).	N/A	N/A	N/A	The RC did not have procedures to identify and mitigate exceedances of identified IROLs and SOLs.
IRO-006-TRE-1	R2.	The RC shall act to identify and mitigate exceedances of identified Interconnection Reliability Operating Limits and System Operating Limits that will not be resolved by the automatic actions of the ERCOT Nodal market operations system, in accordance with the procedures required by R1.	N/A	N/A	The RC failed to follow its procedures in identifying and mitigating an exceedance of an SOL.	The RC failed to follow its procedures in identifying and mitigating an exceedance of an IROL.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-006-WECC-1	R1.	Upon receiving a request of Step 4 or greater (see Attachment 1-IRO-006-WECC-1) from the Transmission Operator of a Qualified Transfer Path, the Reliability Coordinator shall approve (actively or passively) or deny that request within five minutes.	There shall be a Lower Level of non-compliance if there is one instance during a calendar month in which the Reliability Coordinator approved (actively or passively) or denied a Step 4 or greater request greater than five minutes after receipt of notification from the Transmission Operator of a Qualified Transfer Path.	N/A	N/A	N/A
IRO-006-WECC-1	R2.	The Balancing Authorities shall approve curtailment requests to the schedules as submitted, implement alternative actions, or a combination there of that collectively meets the Relief Requirement.	There shall be a Lower Level of non-compliance if there is less than 100% Relief Requirement provided but greater than or equal to 90% Relief Requirement provided or the Relief Requirement was less than 5 MW and was not provided.	There shall be a Moderate Level of non-compliance if there is less than 90% Relief Requirement provided but greater than or equal to 75% Relief Requirement provided and the Relief Requirement was greater than 5 MW and was not provided.	There shall be a High Level of non-compliance if there is less than 75% Relief Requirement provided but greater than or equal to 60% Relief Requirement provided and the Relief Requirement was greater than 5 MW and was not provided.	There shall be a Severe Level of non-compliance if there is less than 60% Relief Requirement provided and the Relief Requirement was greater than 5 MW and was not provided.
IRO-014-1	R1.	The Reliability Coordinator shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability. These Operating Procedures, Processes, or Plans shall address Scenarios	N/A	N/A	The Reliability Coordinator has Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or	The Reliability Coordinator failed to have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that affect other Reliability Coordinator Areas as well as those developed in coordination with other Reliability Coordinators.			coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability, but failed to address Scenarios that affect other Reliability Coordinator Areas.	coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability.
IRO-014-1	R1.1.	These Operating Procedures, Processes, or Plans shall collectively address, as a minimum, the following:	N/A	The Reliability Coordinator failed to include one of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in its Operating Procedures, Processes, or Plans.	The Reliability Coordinator failed to include two of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in its Operating Procedures, Processes, or Plans.	The Reliability Coordinator failed to include more than two of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in its Operating Procedures, Processes, or Plans.
IRO-014-1	R1.1.1.	Communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.2.	Energy and capacity shortages.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.3.	Planned or unplanned outage information.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.4.	Voltage control, including the coordination of reactive resources for voltage control.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.5.	Coordination of information exchange to support reliability assessments.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.6.	Authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-014-1	R2.	Each Reliability Coordinator's Operating Procedure, Process, or Plan that requires one or more other Reliability Coordinators to take action (e.g., make notifications, exchange information, or coordinate actions) shall be:	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R2.1 or R2.2.
IRO-014-1	R2.1.	Agreed to by all the Reliability Coordinators required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not agreed to by all the Reliability Coordinators required to take the indicated action(s).
IRO-014-1	R2.2.	Distributed to all Reliability Coordinators that are required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not distributed to all Reliability Coordinators that are required to take the indicated action(s).
IRO-014-1	R3.	A Reliability Coordinator's Operating Procedures, Processes, or Plans developed to support a Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan shall include:	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R3.1 or R3.2.
IRO-014-1	R3.1.	A reference to the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to reference the

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R3.2.	The agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to include the agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R4.	Each of the Operating Procedures, Processes, and Plans addressed in Reliability Standard IRO-014 Requirement 1 and Requirement 3 shall:	N/A	The Operating Procedures, Processes and Plans did not include **one** of the elements listed in IRO-014-1 R4.1 through R4.3.	The Operating Procedures, Processes and Plans did not include **two** of the elements listed in IRO-014-1 R4.1 through R4.3.	The Operating Procedures, Processes and Plans did not include **any** of the elements listed in IRO-014-1 R4.1 through R4.3.
IRO-014-1	R4.1.	Include version control number or date	N/A	N/A	N/A	N/A
IRO-014-1	R4.2.	Include a distribution list.	N/A	N/A	N/A	N/A
IRO-014-1	R4.3.	Be reviewed, at least once every three years, and updated if needed.	N/A	N/A	N/A	N/A
IRO-015-1	R1.	The Reliability Coordinator shall follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notifications and exchanging reliability-related information with other Reliability Coordinators but no adverse reliability impacts resulted from the incident.		related information with other Reliability Coordinators and adverse reliability impacts resulted from the incident.
IRO-015-1	R1.1.	The Reliability Coordinator shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas.	N/A	The Reliability Coordinator failed to make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas but no adverse reliability impacts resulted from the incident.	N/A	The Reliability Coordinator failed to make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas and adverse reliability impacts resulted from the incident.
IRO-015-1	R2.	The Reliability Coordinator shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.
IRO-015-1	R2.1.	The frequency of these conference calls shall be agreed upon by all involved Reliability Coordinators and shall be at least weekly.	N/A	N/A	N/A	The Reliability Operator failed to participate in the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment of the need and frequency of conference calls with other Reliability Operators.
IRO-015-1	R3.	The Reliability Coordinator shall provide reliability-related information as requested by other Reliability Coordinators.				The Reliability Coordinator failed to provide reliability-related information as requested by other Reliability Coordinators.
IRO-016-1	R1.	The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.	The Reliability Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators, contacted the other Reliability Coordinator(s) to confirm that there was a problem, discussed options and decided upon a solution to prevent or resolve the identified problem, but failed to have evidence that it coordinated with other Reliability Coordinators.	N/A	N/A	The Reliability Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators failed to contact the other Reliability Coordinator(s) to confirm that there was a problem, discuss options and decide upon a solution to prevent or resolve the identified problem.
IRO-016-1	R1.1.	If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall	The responsible entity agreed on the problem and the actions to take to prevent or mitigate	N/A	N/A	The responsible entity agreed on the problem and the actions to take to prevent or mitigate

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.	the system condition, implemented the agreed-upon solution, but failed to notify the involved Reliability Coordinators of the action(s) taken.			the system condition, but failed to implement the agreed-upon solution.
IRO-016-1	R1.2.	If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).	N/A	N/A	N/A	The involved Reliability Coordinators could not agree on the problem(s), but a Reliability Coordinator failed to re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
IRO-016-1	R1.2.1.	If time permits, this re-evaluation shall be done before taking corrective actions.	N/A	N/A	N/A	The Reliability Coordinator failed to re-evaluate the problem prior to taking corrective actions, during periods when time was not an issue.
IRO-016-1	R1.2.2.	If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.	N/A	N/A	N/A	The Reliability Coordinator failed to operate as though the problem(s) exist(s) until the conflicting system status was resolved, during periods when time was an issue.
IRO-016-1	R1.3.	If the involved Reliability Coordinators cannot agree on the solution, the more	N/A	N/A	N/A	The Reliability Coordinator

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		conservative solution shall be implemented.				implemented a solution other than the most conservative solution, when agreement on the solution could not be reached.
IRO-016-1	R2. (Retired)	The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.	N/A	N/A	N/A	The Reliability Coordinator failed to document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

Formatted: Font color: Red

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-010-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to 50% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.
MOD-010-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide this steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. If no schedule exists, then	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the steady-state modeling and simulation data to	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the steady-state modeling	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the steady-state modeling and simulation data to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		these entities shall provide the data on request (30 calendar days).	the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 30 but less than or equal to 35 calendar days following the request.	50% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.	and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 40 but less than or equal to 45 calendar days following the request.	Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide data more than 45 calendar days following the request.
MOD-012-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R1) shall provide appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics and system data in compliance with the respective	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the appropriate equipment characteristics and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the appropriate equipment characteristics and system data in compliance with the	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics and system data in compliance with the respective

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1	system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.
MOD-012-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R4) shall provide dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. If no schedule exists, then these entities shall provide data on request (30 calendar days).	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1 OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule exists, The	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Planners provided data more than 30 but less than or equal to 35 calendar days following the request.	Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.	more than 40 but less than or equal to 45 calendar days following the request.	provide data more than 45 calendar days following the request.
MOD-016-1.1	R1.	The Planning Authority and Regional Reliability Organization shall have documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses.	N/A	The responsible entity did not have documentation identifying the scope and details of the actual and forecast data for one (1) of the following types of data to be reported for system modeling and reliability analyses: • Demand data • Net Energy for Load data • Controllable DSM data	The responsible entity did not have documentation identifying the scope and details of the actual and forecast data for two (2) of the following to be reported for system modeling and reliability analyses: • Demand data • Net Energy for Load data • Controllable DSM data	The responsible entity did not have documentation identifying the scope and details of the actual and forecast data to be reported for system modeling and reliability analyses.
MOD-016-1.1	R1.1.	The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that	The responsible entity failed to ensure that consistent data is supplied for one of the Reliability Standards as specified in R1.1.	The responsible entity failed to ensure that consistent data is supplied for two of the Reliability Standards as specified in R1.1.	The responsible entity failed to ensure that consistent data is supplied for three of the Reliability Standards as specified in R1.1.	The responsible entity failed to ensure that consistent data is supplied for four or more of the Reliability Standards as specified in R1.1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.				OR The responsible entity failed to stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.
MOD-016-1.1	R2.	The Regional Reliability Organization shall distribute its documentation required in Requirement 1 and any changes to that documentation, to all Planning Authorities that work within its Region.	N/A	N/A	The Regional Reliability Organization distributed its documentation as specified in R1 but failed to distribute any changes to that documentation, to all Planning Authorities that work within its Region.	The Regional Reliability Organization failed to distribute its documentation as specified in R1 to all Planning Authorities that work within its Region.
MOD-016-1.1	R2.1.	The Regional Reliability Organization shall make this distribution within 30 calendar days of approval.	The Regional Reliability Organization distributed the documentation more than 30 but less than or equal to 37 calendar days following approval.	The Regional Reliability Organization made the distribution more than 37 but less than or equal to 51 calendar days following approval.	The Regional Reliability Organization made the distribution more than 51 but less than or equal to 58 calendar days following approval.	The Regional Reliability Organization failed to make the distribution more than 58 calendar days following approval.
MOD-016-1.1	R3.	The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and	The responsible entity failed to distribute its documentation required in Requirement R1 and	The responsible entity failed to distribute its documentation required in	The responsible entity failed to distribute its documentation required in Requirement R1 and any changes to that	The responsible entity failed to distribute its documentation as specified in Requirement R1 to

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Load-Serving Entities that work within its Planning Authority Area.	any changes to that documentation to 5% or less of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity distributed the documentation more than 30 calendar days but less than or equal to 40 calendar days following approval.	Requirement R1 and any changes to that documentation to more than 5% up to (and including) 10% of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity made the distribution more than 40 calendar days but less than or equal to 50 calendar days following approval.	documentation to more than 10% up to (and including) 15% of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity made the distribution more than 50 calendar days but less than or equal to 60 calendar days following approval.	more than 15% of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity failed to make the distribution more than 60 calendar days following approval.
MOD-016-1.1	R3.1.	The Planning Authority shall make this distribution within 30 calendar days of approval.	N/A	N/A	N/A	N/A
MOD-017-0.1	R1.	The Load-Serving Entity, Planning Authority, and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R 1.	The responsible entity failed to provide one (1) of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The responsible entity failed to provide two (2) of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The responsible entity failed to provide three (3) of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The responsible entity failed to provide all of the elements of information as specified in R1.1, R1.2, R1.3 and R1.4 on an annual basis.
MOD-017-0.1	R1.1.	Integrated hourly demands in megawatts (MW) for the prior year.	N/A	N/A	N/A	N/A
MOD-017-0.1	R1.2.	Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-017-0.1	R1.3.	Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.	N/A	N/A	N/A	N/A
MOD-017-0.1	R1.4.	Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.	N/A	N/A	N/A	N/A
MOD-018-0	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or dispersed basis) shall:	N/A	The responsible entity's report failed to include one (1) of the items as specified in R1.1, R1.2, or R1.3.	The responsible entity's report failed to include two (2) of the items as specified in R1.1, R1.2, or R1.3.	The responsible entity's report failed to include any of the items as specified in R1.1, R1.2, and R1.3.
MOD-018-0	R1.1.	Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and	N/A	N/A	N/A	N/A
MOD-018-0	R1.2.	Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load.	N/A	N/A	N/A	N/A
MOD-018-0	R1.3.	Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1.	N/A	N/A	N/A	N/A
MOD-018-0	R2.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days).	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to report the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 30 but less than or equal to 45 calendar days following the request.	NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 45 but less than or equal to 60 calendar days following the request.	Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 60 but less than or equal to 75 calendar days following the request.	Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 75 calendar days following the request.
MOD-019-0.1	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R 1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually less than or equal to 25% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 25% but less than or equal to 50% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 50% but less than or equal to 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			MOD-016-0_R 1.	Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.	MOD-016-0_R1.	MOD-016-0_R1.
MOD-020-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 30 but less than 45 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 45 but less than 60 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 60 but less than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to make known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.
MOD-021-1	R1.	The Load-Serving Entity, Transmission Planner and Resource Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed.	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how one (1)	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how three (3) of the following	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts failed to document how the Demand and energy effects of DSM programs are addressed.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	document how two (2) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	
MOD-021-1	R2.	The Load-Serving Entity, Transmission Planner and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R1.	N/A	N/A	N/A	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R 1.
MOD-021-1	R3.	The Load-Serving Entity, Transmission Planner and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days).	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 30 but less than 45 calendar days	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 45 but	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 60 but less than 75 calendar days following	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to provide documentation on the treatment of its DSM programs more than 75 calendar days following the request

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			following the request from NERC.	less than 60 calendar days following the request from NERC.	the request from NERC.	from NERC.

Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-2	R1.	The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt.	The Nuclear Plant Generator Operator provided the NPIR's to the applicable entities but did not verify receipt.	The Nuclear Plant Generator Operator did not provide the proposed NPIR to one of the applicable entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to two of the applicable entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to more than two of applicable entities.
NUC-001-2	R2.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.	N/A	N/A	N/A	The Nuclear Plant Generator Operator or the applicable Transmission Entity does not have in effect one or more agreements that include mutually agreed to NPIRs and document the implementation of the NPIRs.
NUC-001-2	R3.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator.	N/A	The responsible entity incorporated the NPIRs into its planning analyses but did not communicate the results to the Nuclear Plant Generator Operator.	N/A	The responsible entity did not incorporate the NPIRs into its planning analyses of the electric system.
NUC-001-2	R4.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall:	The applicable Transmission Entity failed to incorporate one or more applicable NPIRs into their operating analyses.	The applicable Transmission Entity failed to incorporate any NPIRs into their operating analyses OR did not inform NPG operator when their ability of	The applicable Transmission Entity failed to operate the system to meet the NPIRs	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assess the operation of the electric system affecting the NPIRs was lost.		
NUC-001-2	R4.1	Incorporate the NPIRs into their operating analyses of the electric system.	N/A	N/A	N/A	N/A
NUC-001-2	R4.2	Operate the electric system to meet the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R4.3	Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.	N/A	N/A	N/A	N/A
NUC-001-2	R5.	The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard.	N/A	N/A	N/A	The Nuclear Plant Generator Operator failed to operate per the Agreements developed in accordance with this standard.
NUC-001-2	R6.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs.	The Nuclear Operator or Transmission Entity failed to coordinate outages or maintenance activities in accordance with one or more of the administrative elements within the agreements.	The Nuclear Operator or Transmission Entity failed to provide outage or maintenance schedules to the appropriate parties as described in the agreement or on a time period consistent with the agreements.	The Nuclear Operator or Transmission Entity failed to coordinate one or more outages or maintenance activities in accordance the requirements of the agreements.	N/A
NUC-001-2	R7.	Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design,	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities	The Nuclear Plant Generator Operator did not inform the applicable Transmission	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	of proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	Entities of actual changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	of actual changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that directly impact the ability of the electric system to meet the NPIRs.	
NUC-001-2	R8.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of proposed changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that directly impacts the ability of the electric system to meet the NPIRs.	N/A
NUC-001-2	R9.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2:	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing one or more sub-components of R9.1.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from one to five of the combined sub-	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from six to ten of the combined sub-components in R9.2,	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing eleven or more of the combined sub-components in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Retired)	components in R9.2, R9.3 and R9.4.	R9.3 and R9.4.	R9.2, R9.3 and R9.4.
NUC-001-2	R9.1 (Retired)	Administrative elements:	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.1 (Retired)	Definitions of key terms used in the agreement.	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.2 (Retired)	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.3 (Retired)	A requirement to review the agreement(s) at least every three years.	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.4 (Retired)	A dispute resolution mechanism.	N/A	N/A	N/A	N/A
NUC-001-2	R9.2	Technical requirements and analysis:	N/A	N/A	N/A	N/A
NUC-001-2	R9.2.1	Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.	N/A	N/A	N/A	N/A
NUC-001-2	R9.2.2	Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.2.3	Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3	Operations and maintenance coordination:	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.1	Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and	N/A	N/A	N/A	N/A

Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		responsibilities for operational control coordination and maintenance of these facilities.				
NUC-001-2	R9.3.2	Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.3	Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.4	Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.5	Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.6	Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.7	Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4	Communications and training:	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-2	R9.4.1	Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.2	Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.3	Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.4	Provisions for supplying information necessary to report to government agencies, as related to NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.5	Provisions for personnel training, as related to NPIRs.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-001-0.2	R1.	Each Transmission Operator and Balancing Authority shall provide operating personnel with the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	N/A	N/A	The Transmission Operator or Balancing Authority failed to demonstrate that it communicated to its operating personnel their responsibility or their authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	The Transmission Operator or Balancing Authority failed to demonstrate that it communicated to its operating personnel their responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.
PER-002-0	R1.	Each Transmission Operator and Balancing Authority shall be staffed with adequately trained operating personnel.	The responsible entity failed to staff 5% or less with adequately trained operating personnel.	The responsible failed to staff more than 5% up to (and including) 10% with adequately trained operating personnel.	The responsible entity failed to staff more than 10% up to (and including) 15% with adequately trained operating personnel.	The responsible entity failed to staff more than 15% with adequately trained operating personnel.
PER-002-0	R2.	Each Transmission Operator and Balancing Authority shall have a training program for all operating personnel that are in:	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting 5% or less of its operating personnel.	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting more than 5% up to (and including) 10% of its operating personnel.	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting more than 10% up to (and including) 15% of its operating personnel.	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting more than 15% of its operating personnel.
PER-002-0	R2.1.	Positions that have the primary responsibility, either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System.	N/A	N/A	N/A	N/A
PER-002-0	R2.2.	Positions directly responsible for complying with NERC standards.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-002-0	R3.	For personnel identified in Requirement R2, the Transmission Operator and Balancing Authority shall provide a training program meeting the following criteria:	The applicable entity did not comply with one of the four required elements.	The applicable entity did not comply with two of the four required elements.	The applicable entity did not comply with three of the four required elements.	The applicable entity did not comply with any of the four required elements.
PER-002-0	R3.1.	A set of training program objectives must be defined, based on NERC and Regional Reliability Organization standards, entity operating procedures, and applicable regulatory requirements. These objectives shall reference the knowledge and competencies needed to apply those standards, procedures, and requirements to normal, emergency, and restoration conditions for the Transmission Operator and Balancing Authority operating positions.	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for less than 25% of the applicable BA and TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 25% or more but less than 50% of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 50% or more but less than 75% of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 75% or more of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)
PER-002-0	R3.2.	The training program must include a plan for the initial and continuing training of Transmission Operator and Balancing Authority operating personnel. That plan shall address knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			knowledge and competencies required for reliable system operations.	knowledge and competencies required for reliable system operations.		
PER-002-0	R3.3.	The training program must include training time for all Transmission Operator and Balancing Authority operating personnel to ensure their operating proficiency.	The responsible entity has produced the training program with more than 75% but less than 100% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 50% but less than or equal to 75% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 25% but less than or equal to 50% of operating personnel provided with training time.	The responsible entity has produced the training program with more than or equal to 0% but less than or equal to 25% of operating personnel provided with training time.
PER-002-0	R3.4.	Training staff must be identified, and the staff must be competent in both knowledge of system operations and instructional capabilities.	N/A	The responsible entity has produced the training program with training staff identified that lacks knowledge of system operations. OR The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	The responsible entity has produced the training program with training staff identified that lacks knowledge of system operations. AND The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	The responsible entity has produced the training program with no training staff identified.
PER-003-1	R1.	Each Reliability Coordinator shall staff its Real-time operating positions performing Reliability Coordinator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining a valid NERC Reliability Operator				The Reliability Coordinator failed to staff each Real-time operating position performing Reliability Coordinator reliability-related

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		certificate:				tasks with a System Operator having a valid NERC certificate as defined in Requirement R1.
PER-003-1	R2.	Each Transmission Operator shall staff its Real-time operating positions performing Transmission Operator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates:				The Transmission Operator failed to staff each Real-time operating position performing Transmission Operator reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R2, Part 2.2.
PER-003-1	R3.	Each Balancing Authority shall staff its Real-time operating positions performing Balancing Authority reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates:				The Balancing Authority failed to staff each Real-time operating position performing Balancing Authority reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R3, Part 3.2.

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-004-1	R3.	Reliability Coordinator operating personnel shall have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	5% or less of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	More than 5% up to (and including) 10% of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	More than 10% up to (and including) 15% of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	More than 15% of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.
PER-004-1	R4.	Reliability Coordinator operating personnel shall have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.	5% or less of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and	More than 5% up to (and including) 10% of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment	More than 10% up to (and including) 15% of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.	More than 15% of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			operational restrictions.	capabilities, and operational restrictions.		

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-001-1	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.	N/A	N/A	The responsible entity failed to be familiar with the limitations of protection system schemes applied in its area.	The responsible entity failed to be familiar with the purpose of protection system schemes applied in its area.
PRC-001-1	R2.	Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:	N/A	N/A	N/A	The responsible entity failed to notify any reliability entity of relay or equipment failures.
PRC-001-1	R2.1.	If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, but corrective action was taken.	Notification of relay or equipment failure was made to the Transmission Operator and Host Balancing Authority, but corrective action was not taken.	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, and corrective action was not taken.
PRC-001-1	R2.2.	If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing Authorities, but corrective action was taken.	Notification of relay or equipment failure was made to the Reliability Coordinator and affected Transmission Operators and Balancing Authorities, but corrective action was not taken.	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing Authorities, and corrective action was not taken.
PRC-001-1	R3.	A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-001-1	R3.1.	Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.	The Generator Operator failed to coordinate one new protective system or protective system change with either its Transmission Operator or its Host Balancing Authority or both.	The Generator Operator failed to coordinate two new protective systems or protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate three new protective systems or protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate more than three new protective systems or protective system changes with its Transmission Operator or its Host Balancing Authority, or both.
PRC-001-1	R3.2.	Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate one new protective system or protective system change with neighboring Transmission Operators or Balancing Authorities or both.	The Transmission Operator failed to coordinate two new protective systems or protective system changes with neighboring Transmission Operators or Balancing Authorities or both.	The Transmission Operator failed to coordinate three new protective systems or protective system changes with neighboring Transmission Operators or Balancing Authorities or both.	The Transmission Operator failed to coordinate more than three new protective systems or protective system changes with neighboring Transmission Operators or Balancing Authorities or both.
PRC-001-1	R4.	Each Transmission Operator shall coordinate protection systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with one of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with two of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with three of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with three or more of its neighboring Generator Operators, Transmission Operators, and Balancing Authorities.
PRC-001-1	R5.	A Generator Operator or Transmission Operator shall coordinate changes in	N/A	N/A	The Generator Operator failed to notify its	The Generator Operator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		generation, transmission, load or operating conditions that could require changes in the protection systems of others:			Transmission Operator at all of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems. (R5.1) OR The Transmission Operator failed to notify neighboring Transmission Operators at all of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems. (R5.2)	notify its Transmission Operator at all of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems. (R5.1) AND The Transmission Operator failed to notify neighboring Transmission Operators at all of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems. (R5.2)
PRC-001-1	R5.1.	Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.	N/A	N/A	N/A	N/A
PRC-001-1	R5.2.	Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.	N/A	N/A	N/A	N/A
PRC-001-1	R6.	Each Transmission Operator and Balancing Authority shall monitor the status of each	N/A	N/A	The responsible entity monitored the status of	The responsible entity failed to monitor the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.			each Special Protection System in its area but notification of a change in status of a Special Protection System was not made to the affected Transmission Operators and Balancing Authorities.	status of each Special Protection System in its area, and did not notify affected Transmission Operators and Balancing Authorities of each change in status.
PRC-002-NPCC-01	R1.	Each Transmission Owner and Generator Owner shall provide Sequence of Event (SOE) recording capability by installing Sequence of Event recorders or as part of another device, such as a Supervisory Control And Data Acquisition (SCADA) Remote Terminal Unit (RTU), a generator plant Digital (or Distributed) Control System (DCS) or part of Fault recording equipment. This capability shall: [See standard for requirements of SOE recording capability]	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed up to and including 10% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed more than 10% and up to and including 20% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed more than 20% and up to and including 30% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed more than 30% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.
PRC-002-NPCC-01	R2.	Each Transmission Owner shall provide Fault recording capability for the following Elements at facilities where Fault recording equipment is required to be installed as per R3: [See standard for list of elements]	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed up to and including 10% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the criteria listed in 2.1 through 2.6.	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed more than 10% and up to and including 20% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed more than 20% and up to and including 30% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the criteria listed in 2.1 through 2.6.	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed more than 30% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the criteria listed in 2.1 through 2.6.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				criteria listed in 2.1 through 2.6.		
PRC-002-NPCC-01	R3.	Each Transmission Owner shall have Fault recording capability that determines the Current Zero Time for loss of Bulk Electric System (BES) transmission Elements.	N/A	N/A	N/A	The Transmission Owner failed to provide fault recording capability that determines the current zero time for loss of transmission Elements.
PRC-002-NPCC-01	R4.	Each Generator Owner shall provide Fault recording capability for Generating Plants at and above 200 MVA Capacity and connected through a generator step up (GSU) transformer to a Bulk Electric System Element unless Fault recording capability is already provided by the Transmission Owner.	The Generator Owner failed to provide Fault recording capability at up to and including 10% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.	The Generator Owner failed to provide Fault recording capability at more than 10% and up to and including 20% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.	The Generator Owner failed to provide Fault recording capability at more than 20% and up to 30% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.	The Generator Owner failed to provide Fault recording capability at more than 30% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.
PRC-002-NPCC-01	R5.	Each Transmission Owner and Generator Owner shall record for Faults, sufficient electrical quantities for each monitored Element to determine the following: [See standard for list]	The Transmission Owner or Generator Owner failed to record for the Faults up to and including 10% of the total set of parameters, which is the product of the total number of monitored Elements and the number of parameters	The Transmission Owner or Generator Owner failed to record for the Faults more than 10% and up to and including 20% of the total set of parameters, which is the product of the total number of monitored Elements	The Transmission Owner or Generator Owner failed to record for the Faults more than 20% and up to and including 30% of the total set of parameters, which is the product of the total number of monitored Elements and the number of parameters	The Transmission Owner or Generator Owner failed to record for the Faults more than 30% of the total set of parameters, which is the product of the total number of monitored Elements and the number of parameters listed in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			listed in 5.1 through 5.5.	and the number of parameters listed in 5.1 through 5.5.	listed in 5.1 through 5.5.	5.1 through 5.5.
PRC-002-NPCC-01	R6.	Each Transmission Owner and Generator Owner shall provide Fault recording with the following capabilities: [See standard for list of capabilities]	The Transmission Owner or Generator Owner failed to provide Fault recording capability for up to and including 10% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of capabilities identified in 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for up to 2 locations.	The Transmission Owner or Generator Owner failed to provide Fault recording capability for more than 10% and up to and including 20% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of capabilities identified in 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for more than two (2) and up to and including five (5) locations.	The Transmission Owner or Generator Owner failed to provide Fault recording capability for more than 20% and up to and including 30% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for more than five (5) and up to and including ten (10) locations.	The Transmission Owner or Generator Owner failed to provide Fault recording capability for more than 30% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of capabilities identified in 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for more than ten (10) locations.
PRC-002-NPCC-01	R7.	Each Reliability Coordinator shall establish its area's requirements for Dynamic Disturbance Recording (DDR) capability that: [See standard for futher requirements]	The Reliability Coordinator failed to establish its area's requirements for up to and including 10% of the required DDR	The Reliability Coordinator failed to establish its area's requirements for more than 10% and up to and including	The Reliability Coordinator failed to establish its area's requirements for more than 20% and up to and including 30% of the	The Reliability Coordinator failed to establish its area's requirements for more than 30% of the required DDR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			coverage for its area as per 7.1and 7.2.	20% of the required DDR coverage for its area as per 7.1 and 7.2.	required DDR coverage for its area as per 7.1 and 7.2.	coverage for its area as per 7.1 and 7.2.
PRC-002-NPCC-01	R8.	Each Reliability Coordinator shall specify that DDRs installed, after the approval of this standard, function as continuous recorders.	N/A	N/A	N/A	The Reliability Coordinator failed to specify that DDRs installed function as continuous recorders.
PRC-002-NPCC-01	R9.	Each Reliability Coordinator shall specify that DDRs are installed with the following capabilities: [See standard for list of capabilities]	N/A	N/A	N/A	The Reliability Coordinator failed to specify that DDRs are installed without the capabilities listed in 9.1 through 9.3.
PRC-002-NPCC-01	R10.	Each Reliability Coordinator shall establish requirements such that the following quantities are monitored or derived where DDRs are installed: [See standard for quantities]	N/A	N/A	N/A	The Reliability Coordinator failed to ensure that the quantities listed in 10.1 through 10.5 are monitored or derived where DDRs are installed.
PRC-002-NPCC-01	R11.	Each Reliability Coordinator shall document additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10, and report this to the Regional Entity (RE) upon request.	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for up to two (2) facilities within the Reliability Coordinator's area	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for more than two (2) and up to five (5)	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for more than five (5) and up to ten (10) facilities within the Reliability Coordinator's area that have a DDR.	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for more than ten (10) facilities within the Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			that have a DDR.	facilities within the Reliability Coordinator's area that have a DDR.		Coordinator's area that have a DDR.
PRC-002-NPCC-01	R12.	Each Reliability Coordinator shall specify its DDR requirements including the DDR setting triggers established in R9 to the Transmission Owners and Generator Owners.	N/A	N/A	N/A	The Reliability Coordinator failed to specify to the Transmission Owners and Generator Owners its DDR requirements including the DDR setting triggers established in R9 but missed established setting triggers.
PRC-002-NPCC-01	R13.	Each Transmission Owner and Generator Owner that receives a request from the Reliability Coordinator to install a DDR shall acquire and install the DDR in accordance with R12. Reliability Coordinators, Transmission Owners, and Generator Owners shall mutually agree on an implementation schedule.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for up to and including 10% of the requirement set of the Reliability Coordinator's request to install DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for more than 10% and up to 20% of the requirement set requested by the Reliability Coordinator for installing DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for more than 20% and up to 30% of the requirement set requested by the Reliability Coordinator for installing DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for more than 30% of the requirement set requested by the Reliability Coordinator and installing DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Reliability Coordinator, Transmission Owners, and Generator Owners failed to mutually agree on an implementation schedule.
PRC-002-NPCC-01	R14.	Each Transmission Owner and Generator Owner shall establish a maintenance and testing program for stand alone DME (equipment whose only purpose is disturbance monitoring) that includes: [See standard for list of inclusions]	The Transmission Owner or Generator Owner established a maintenance and testing program for stand alone DME but provided incomplete data for any one (1) of 14.1 through 14.7.	The Transmission Owner or Generator Owner established a maintenance and testing program for stand alone DME but provided incomplete data for more than one (1) and up to and including three (3) of 14.1 through 14.7.	The Transmission Owner or Generator Owner established a maintenance and testing program for stand alone DME but provided incomplete data for more than three (3) and up to and including six (6) of 14.1 through 14.7.	The Transmission Owner or Generator Owner did not establish any maintenance and testing program for DME; OR The Transmission Owner or Generator Owner established a maintenance and testing program for DME but did not provide any data that meets all of 14.1 through 14.7.
PRC-002-NPCC-01	R15.	Each Reliability Coordinator, Transmission Owner and Generator Owner shall share data within 30 days upon request. Each Reliability Coordinator, Transmission Owner, and Generator Owner shall provide recorded disturbance data from DMEs within 30 days of receipt of the request in each of the following cases: [See standard for the two cases]	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for up to and including fifteen (15) days in	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for more than fifteen (15) days but	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for more than 30 days but less than and including	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for more than forty-five (45) days in meeting

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			meeting the requests of an entity, or entities in 15.1, or 15.2.	less than and including thirty (30) days in meeting the requests of an entity, or entities in 15.1 or 15.2.	forty-five (45) days in meeting the requests of an entity, or entities in 15.1 or 15.2.	the requests of an entity, or entities in 15.1 or 15.2.
PRC-002-NPCC-01	R16.	Each Reliability Coordinator, Transmission Owner and Generator Owner shall submit the data files conforming to the following format requirements: [See standard for format requirements]	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit up to and including two (2) data files in a format that meets the applicable format requirements in 16.1 through 16.3.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit more than two (2) and up to and including five (5) data files in a format that meets the applicable format requirements in 16.1 through 16.3.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit more than five (5) and up to and including ten (10) data files in a format that meets the applicable format requirements in 16.1 through 16.3.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit more than ten (10) data files in a format that meets the applicable format requirements in 16.1 through 16.3.
PRC-002-NPCC-01	R17.	Each Reliability Coordinator, Transmission Owner and Generator Owner shall maintain, record and provide to the Regional Entity (RE), upon request, the following data on the DMEs installed to meet this standard: [See standard for types of data]	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request up to and including two (2) of the items in 17.1 through 17.8.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request more than two (2) and up to and including four (4) of the items in 17.1 to 17.8.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request more than four (4) and up to and including six (6) of the items in 17.1 through 17.8.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request more than six (6) of the items in 17.1 through 17.8.
PRC-004-1a	R1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid	N/A	The responsible entity provided evidence of analyzing a Misoperation but the documentation and	N/A	The responsible entity did not perform an analysis of a Misoperation.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for Reliability Standard PRC-003 Requirement 1.		implementation of the associated Corrective Action Plan was not provided.		
PRC-004-1a	R2.	The Generator Owner shall analyze its generator Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	N/A	The Generator Owner provided evidence of analyzing a Misoperation but the documentation and implementation of the associated Corrective Action Plan was not provided.	N/A	The Generator Owner did not perform an analysis of a Misoperation.
PRC-004-1a	R3.	The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its Regional Reliability Organization, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses and its Corrective Action Plans, but did not provide these according to the Regional Reliability Organization's procedures.	N/A	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses but did not provide its Corrective Action Plans.	The responsible entity did not provide its Regional Reliability Organization with documentation of its Misoperations analyses and did not provide its Corrective Action Plans.
PRC-004-2a	R1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		according to the Regional Entity's procedures.				
PRC-004-2a	R2.	The Generator Owner shall analyze its generator Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Entity's procedures.	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed
PRC-004-2a	R3.	The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its Regional Entity, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Entity's procedures.	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses and its Corrective Action Plans, but did not provide these according to the Regional Reliability Organization's procedures.	N/A	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses but did not provide its Corrective Action Plans.	The responsible entity did not provide its Regional Reliability Organization with documentation of its Misoperations analyses and did not provide its Corrective Action Plans.
PRC-004-WECC-1	R1.	System Operators and System Protection personnel of the Transmission Owners and Generator Owners shall analyze all Protection System and RAS operations.	System Operating personnel of the Transmission Owner or Generator Owner did not review the Protection System Operation or RAS operation within 24 hours but did review the Protection System Operation or RAS operation within six business days.	System Operating personnel of the Transmission Owner or Generator Owner did not review the Protection System operation or RAS operation within six business days.	System Protection personnel of the Transmission Owner and Generator Owner did not analyze the Protection System operation or RAS operation within 20 business days but did analyze the Protection System operation or RAS operation within 25 business days.	System Protection personnel of the Transmission Owner or Generator Owner did not analyze the Protection System operation or RAS operation within 25 business days.
PRC-004-	R1.1.	System Operators shall review all tripping of transmission elements and RAS operations to				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
WECC-1		identify apparent Misoperations within 24 hours.				
PRC-004-WECC-1	R1.2.	System Protection personnel shall analyze all operations of Protection Systems and RAS within 20 business days for correctness to characterize whether a Misoperation has occurred that may not have been identified by System Operators.				
PRC-004-WECC-1	R2.	Transmission Owners and Generator Owners shall perform the following actions for each Misoperation of the Protection System or RAS. It is not intended that Requirements R2.1 through R2.4 apply to Protection System and/or RAS actions that appear to be entirely reasonable and correct at the time of occurrence and associated system performance is fully compliant with NERC Reliability Standards. If the Transmission Owner or Generator Owner later finds the Protection System or RAS operation to be incorrect through System Protection personnel analysis, the requirements of R2.1 through R2.4 become applicable at the time the Transmission Owner or Generator Owner identifies the Misoperation:				
PRC-004-WECC-1	R2.1.	If the Protection System or RAS has a Security-Based Misoperation and two or more Functionally Equivalent Protection Systems (FEPS) or Functionally Equivalent RAS (FERAS) remain in service to ensure Bulk Electric System (BES) reliability, the Transmission Owners or Generator Owners shall remove from service the Protection System or RAS that misoperated within 22 hours following identification of the Misoperation. Repair or replacement of the failed Protection System or RAS is at the	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 22 hours but did perform the requirements	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 24 hours but did	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 28 hours but did perform the requirements within	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 32 hours.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Owners' and Generator Owners' discretion.	within 24 hours.	perform the requirements within 28 hours.	32 hours.	
PRC-004-WECC-1	R2.2.	If the Protection System or RAS has a Security-Based Misoperation and only one FEPS or FERAS remains in service to ensure BES reliability, the Transmission Owner or Generator Owner shall perform the following.				
PRC-004-WECC-1	R2.2.1.	Following identification of the Protection System or RAS Misoperation, Transmission Owners and Generator Owners shall remove from service within 22 hours for repair or modification the Protection System or RAS that misoperated.	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 22 hours but did perform the requirements within 24 hours.	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 24 hours but did perform the requirements within 28 hours.	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 28 hours but did perform the requirements within 32 hours.	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 32 hours.
PRC-004-WECC-1	R2.2.2.	The Transmission Owner or Generator Owner shall repair or replace any Protection System or RAS that misoperated with a FEPS or FERAS within 20 business days of the date of removal. The Transmission Owner or Generator Owner shall remove the Element from service or disable the RAS if repair or replacement is not completed within 20 business days.	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustments to comply with the requirements within 20 business days but did perform the required activities within 25 business days.	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustment to comply with the requirements within 25 business days but did perform the required activities	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustment to comply with the requirements within 28 business days but did perform the required activities within 30 business days.	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustments to comply with the requirements within 30 business days.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within 28 business days.		
PRC-004-WECC-1	R2.3.	If the Protection System or RAS has a Security-Based or Dependability-Based Misoperation and a FEPS and FERAS is not in service to ensure BES reliability, Transmission Owners or Generator Owners shall repair and place back in service within 22 hours the Protection System or RAS that misoperated. If this cannot be done, then Transmission Owners and Generator Owners shall perform the following.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required within 22 hours but did perform the requirements within 24 hours.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 24 hours but did perform the requirements within 28 hours.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 28 hours but did perform the requirements within 32 hours.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required within 32 hours.
PRC-004-WECC-1	R2.3.1.	When a FEPS is not available, the Transmission Owners shall remove the associated Element from service.				
PRC-004-WECC-1	R2.3.2.	When FERAS is not available, then				
PRC-004-WECC-1	R2.3.2.1.	The Generator Owners shall adjust generation to a reliable operating level, or				
PRC-004-WECC-1	R2.3.2.2.	Transmission Operators shall adjust the SOL and operate the facilities within established limits.				
PRC-004-WECC-1	R2.4.	If the Protection System or RAS has a Dependability-Based Misoperation but has one or more FEPS or FERAS that operated correctly, the associated Element or	The Transmission Owner and Generator Owner did not perform the required	The Transmission Owner and Generator Owner did not perform the	The Transmission Owner and Generator Owner did not perform the required repairs,	The Transmission Owner and Generator Owner did not perform the required

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission path may remain in service without removing from service the Protection System or RAS that failed, provided one of the following is performed.	repairs, replacement, or system operation adjustments to comply with the requirements within 20 business days but did perform the required activities within 25 business days.	required repairs, replacement, or system operation adjustment to comply with the requirements within 25 business days but did perform the required activities within 28 business days.	replacement, or system operation adjustment to comply with the requirements within 28 business days but did perform the required activities within 30 business days.	repairs, replacement, or system operation adjustments to comply with the requirements within 30 business days.
PRC-004-WECC-1	R2.4.1.	Transmission Owners or Generator Owners shall repair or replace any Protection System or RAS that misoperated with FEPS and FERAS within 20 business days of the date of the Misoperation identification, or				
PRC-004-WECC-1	R2.4.2.	Transmission Owners or Generator Owners shall remove from service the associated Element or RAS.				
PRC-004-WECC-1	R3.	Transmission Owners and Generation Owners shall submit Misoperation incident reports to WECC within 10 business days for the following.				
PRC-004-WECC-1	R3.1.	Identification of a Misoperation of a Protection System and/or RAS,	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 10 business days but did perform the required activities within 15 business days.	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 15 business days but did perform the required activities within 20 business days.	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 20 business days but did perform the required activities within 25 business days.	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 25 business days.

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-004-WECC-1	R3.2.	Completion of repairs or the replacement of Protection System and/or RAS that misoperated.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 10 business days of the completion but did perform the required activities within 15 business days.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 15 business days of the completion but did perform the required activities within 20 business days.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 20 business days of the completion but did perform the required activities within 25 business days.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 25 business days of the completion.
PRC-005-1b	R1.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:	N/A	The responsible entity-had a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES, but the summary of maintenance and testing procedures was missing or incomplete. (R1.2)	The responsible entity had a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES, but the maintenance and testing intervals and their basis were missing or incomplete. (R1.1)	The responsible entity failed to have Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES.
PRC-005-1b	R1.1.	Maintenance and testing intervals and their basis.	N/A	N/A	N/A	N/A
PRC-005-1b	R1.2.	Summary of maintenance and testing procedures.	N/A	N/A	N/A	N/A
PRC-005-1b	R2.	Each Transmission Owner and any Distribution Provider that owns a	The responsible entity provided	Evidence Protection System devices were	Evidence Protection System devices were	Evidence Protection System devices were

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:	documentation of its Protection System maintenance and testing program more than 30 calendar days following a request from its Regional Reliability Organization and/or NERC. OR Evidence Protection System devices were maintained and tested within the defined intervals (R2.1 and R2.2) was missing 5% or less of the applicable devices.	maintained and tested within the defined intervals (R2.1 and R2.2) was missing more than 5% up to (and including) 10% of the applicable devices.	maintained and tested within the defined intervals (R2.1 and R2.2) was missing more than 10% up to (and including) 15% of the applicable devices.	maintained and tested within the defined intervals (R2.1 and R2.2) was missing more than 15% of the applicable devices.
PRC-005-1b	R2.1.	Evidence Protection System devices were maintained and tested within the defined intervals.	N/A	N/A	N/A	N/A
PRC-005-1b	R2.2.	Date each Protection System device was last tested/maintained.	N/A	N/A	N/A	N/A
PRC-006-1	R1.	Each Planning Coordinator shall develop and document criteria, including consideration of historical events and system studies, to select portions of the Bulk Electric System (BES), including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas that may form islands.	N/A	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events and system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas,	The Planning Coordinator failed to develop and document criteria to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				and Regional Entity areas that may form islands. OR The Planning Coordinator developed and documented criteria but failed to include the consideration of system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.	that may form islands.	
PRC-006-1	R2.	Each Planning Coordinator shall identify one or more islands to serve as a basis for designing its UFLS program including: *[See Standard pdf for further information]*	N/A	The Planning Coordinator identified an island(s) to serve as a basis for designing its UFLS program but failed to include one (1) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	The Planning Coordinator identified an island(s) to serve as a basis for designing its UFLS program but failed to include two (2) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	The Planning Coordinator identified an island(s) to serve as a basis for designing its UFLS program but failed to include all of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3. OR The Planning Coordinator failed to identify any island(s) to serve as a basis for designing its UFLS

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						program.
PRC-006-1	R3.	Each Planning Coordinator shall develop a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from an imbalance scenario, where an imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s). *[See Standard pdf for further information]*	N/A	The Planning Coordinator developed a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet one (1) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet two (2) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s).,but failed to meet all the performance characteristic in Requirement R3, Parts 3.1, 3.2, and 3.3 in simulations of underfrequency conditions. OR The Planning Coordinator failed to develop a UFLS program including notification of and a schedule for implementation by UFLS entities within its area
PRC-006-1	R4.	Each Planning Coordinator shall conduct and document a UFLS design assessment at least once every five years that determines	The Planning Coordinator	The Planning Coordinator conducted and	The Planning Coordinator conducted and documented a UFLS	The Planning Coordinator

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2. The simulation shall model each of the following: *[See Standard pdf for further information]*	conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include one (1) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include two (2) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include three (3) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 but simulation failed to include four (4) or more of the items as specified in Requirement R4, Parts 4.1 through 4.7. OR The Planning Coordinator failed to conduct and document a UFLS assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2
PRC-006-1	R5.	Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning	N/A	N/A	N/A	The Planning Coordinator, whose area or portions of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall coordinate its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island through one of the following: • Develop a common UFLS program design and schedule for implementation per Requirement R3 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or • Conduct a joint UFLS design assessment per Requirement R4 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or • Conduct an independent UFLS design assessment per Requirement R4 for the identified island, and in the event the UFLS design assessment fails to meet Requirement R3, identify modifications to the UFLS program(s) to meet Requirement R3 and report these modifications as recommendations to the other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island and the ERO.				whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, failed to coordinate its UFLS program design through one of the manners described in Requirement R5.
PRC-006-1	R6.	Each Planning Coordinator shall maintain a UFLS database containing data necessary to model its UFLS program for use in event analyses and assessments of the UFLS program at least once each calendar year, with no more than 15 months between maintenance activities.	N/A	N/A	N/A	The Planning Coordinator failed to maintain a UFLS database for use in event analyses and assessments of the UFLS program at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						once each calendar year, with no more than 15 months between maintenance activities.
PRC-006-1	R7.	Each Planning Coordinator shall provide its UFLS database containing data necessary to model its UFLS program to other Planning Coordinators within its Interconnection within 30 calendar days of a request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 30 calendar days and up to and including 40 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 40 calendar days but less than and including 50 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 50 calendar days but less than and including 60 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 60 calendar days following the request. OR The Planning Coordinator failed to provide its UFLS database to other Planning Coordinators.
PRC-006-1	R8.	Each UFLS entity shall provide data to its Planning Coordinator(s) according to the format and schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 5 calendar days but less than or equal to 10 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 10 calendar days but less than or equal to 15 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR	The UFLS entity provided data to its Planning Coordinator(s) more than 15 calendar days but less than or equal to 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR The UFLS entity failed to provide data

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The UFLS entity provided data to its Planning Coordinator(s) but the data was not according to the format specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.		to its Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.
PRC-006-1	R9.	Each UFLS entity shall provide automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by its Planning Coordinator(s) in each Planning Coordinator area in which it owns assets.	The UFLS entity provided less than 100% but more than (and including) 95% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.	The UFLS entity provided less than 95% but more than (and including) 90% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.	The UFLS entity provided less than 90% but more than (and including) 85% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.	The UFLS entity provided less than 85% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.
PRC-006-1	R10.	Each Transmission Owner shall provide automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 100% but more than (and including) 95% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if	The Transmission Owner provided less than 95% but more than (and including) 90% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-	The Transmission Owner provided less than 90% but more than (and including) 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS	The Transmission Owner provided less than 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by the UFLS program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission	voltage if required by the UFLS program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission	program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission	for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission
PRC-006-1	R11.	Each Planning Coordinator, in whose area a BES islanding event results in system frequency excursions below the initializing set points of the UFLS program, shall conduct and document an assessment of the event within one year of event actuation to evaluate: *[See Standard pdf for further information]*	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than one year but less than or equal to 13 months of actuation.	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 13 months but less than or equal to 14 months of actuation.	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 14 months but less than or equal to 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate one (1) of the Parts as specified in Requirement R11, Parts11.1 or 11.2.	excursions below the initializing set points of the UFLS program, failed to conduct and document an assessment of the event and evaluate the Parts as specified in Requirement R11, Parts 11.1 and 11.2. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate all of the Parts as specified in Requirement R11, Parts 11.1 and 11.2.
PRC-006-1	R12.	Each Planning Coordinator, in whose islanding event assessment (per R11) UFLS program deficiencies are identified, shall conduct and document a UFLS design assessment to consider the identified deficiencies within two years of event actuation.	N/A	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				design assessment to consider the identified deficiencies greater than two years but less than or equal to 25 months of event actuation.	design assessment to consider the identified deficiencies greater than 25 months but less than or equal to 26 months of event actuation.	design assessment to consider the identified deficiencies greater than 26 months of event actuation. OR The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, failed to conduct and document a UFLS design assessment to consider the identified deficiencies.
PRC-006-1	R13.	Each Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, shall coordinate its event assessment (in accordance with Requirement R11) with all other Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event through one of the following: • Conduct a joint event assessment per Requirement R11 among the Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or • Conduct an independent event assessment per Requirement R11 that	N/A	N/A	N/A	The Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, failed to coordinate its UFLS event assessment with all other Planning Coordinators whose

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reaches conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or • Conduct an independent event assessment per Requirement R11 and where the assessment fails to reach conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, identify differences in the assessments that likely resulted in the differences in the conclusions and recommendations and report these differences to the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event and the ERO.				areas or portions of whose areas were also included in the same islanding event in one of the manners described in Requirement R13
PRC-006-1	R14.	Each Planning Coordinator shall respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the following: *[See Standard pdf for further information]*	N/A	N/A	N/A	The Planning Coordinator failed to respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes were made or reasons why changes were not made to the

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						items in Parts 14.1 through 14.3.
PRC-007-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall ensure that its UFLS program is consistent with its Regional Reliability Organization's UFLS program requirements.	The evaluation of the entity's UFLS program for consistency with its Regional Reliability Organization's UFLS program is incomplete or inconsistent in one or more of the Regional Reliability Organization program requirements, but is consistent with the required amount of load shedding.	The amount of load shedding is less than 95 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 90 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 85 percent of the Regional requirement in any of the load steps.
PRC-007-0	R2.	The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database.	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database but its annual update was late by 30 calendar days or less.	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database but its annual update was late by more than 30 calendar days but less than or equal to 40 calendar days	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database but its annual update was late by more than 40 calendar days but less than or equal to 50 calendar days.	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) did not provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database, OR The responsible entity's annual update was late by more than 50 calendar days.

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-007-0	R3.	The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days).	The responsible entity has provided the documentation in more than 30 calendar days but less than or equal to 40 calendar days.	The responsible entity has provided the documentation in more than 40 calendar days but less than or equal to 50 calendar days.	The responsible entity has provided the documentation in more than 50 calendar days but less than or equal to 60 calendar days.	The responsible entity has not provided the documentation for more than 60 calendar days.
PRC-008-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.	The UFLS equipment identification, testing schedule or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing 5% or less of the applicable equipment.	The UFLS equipment identification, testing schedule, or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing for more than 5% up to (and including) 10% of the applicable equipment.	The UFLS equipment identification, testing schedule, or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing more than 10% up to (and including) 15% of the applicable equipment.	The responsible entity failed to implement UFLS equipment maintenance and testing program. OR The UFLS equipment identification, testing schedule, or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing more than 15% of the applicable equipment.
PRC-008-0	R2.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UFLS equipment maintenance and testing program more than 30 calendar days following a request from its Regional Reliability Organization and/or NERC.	Evidence UFLS equipment was maintained and tested within the defined intervals was missing for more than 5% up to (and including) 10% of the applicable devices.	Evidence UFLS equipment was maintained and tested within the defined intervals was missing for more than 10% up to (and including) 15% of the applicable devices.	Evidence UFLS equipment was maintained and tested within the defined intervals was missing for more than 15% of the applicable devices.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR Evidence UFLS equipment was maintained and tested within the defined intervals was missing for 5% or less of the applicable devices.			
PRC-009-0	R1.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:	The responsible entity that owns or operates a UFLS program failed to include one of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.	The responsible entity that owns or operates a UFLS program failed to include two of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.	The responsible entity that owns or operates a UFLS program failed to include three of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.	The responsible entity that owns or operates a UFLS program failed to conduct an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.1.	A description of the event including initiating conditions.	N/A	N/A	N/A	N/A
PRC-009-0	R1.2.	A review of the UFLS set points and tripping times.	N/A	N/A	N/A	N/A
PRC-009-0	R1.3.	A simulation of the event.	N/A	N/A	N/A	N/A
PRC-009-0	R1.4.	A summary of the findings.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-009-0	R2.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.	The responsible entity has provided the documentation in more than 90 calendar days but less than 105 calendar days.	The responsible entity has provided the documentation in more than 105 calendar days but less than 129 calendar days.	The responsible entity has provided the documentation in more than 129 calendar days but less than 145 calendar days.	The responsible entity has provided the documentation in 145 calendar days or more.
PRC-010-0	R1.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).	The responsible entity conducted an assessment of the effectiveness of its UVLS system within 5 years or as required by changes in system conditions but did not include the associated Transmission Planner(s) and Planning Authority(ies).	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 5 years but did in less than or equal to 6 years. OR The assessment of the effectiveness of the responsible entity's UVLS system did not address one of the elements in R1 (R1.1.1 through R1.1.3).	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 6 years but did in less than or equal to 7years. OR The assessment of the effectiveness of the responsible entity's UVLS system did not address two of the elements in R1 (R1.1.1 through R1.1.3).	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 7 years. OR The assessment of the effectiveness of the responsible entity's UVLS system did not address any of the elements in R1 (R1.1.1 through R1.1.3).
PRC-010-0	R1.1.	This assessment shall include, but is not limited to:	N/A	N/A	N/A	N/A
PRC-010-0	R1.1.1.	Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-010-0	R1.1.2.	Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.	N/A	N/A	N/A	N/A
PRC-010-0	R1.1.3.	A review of the voltage set points and timing.	N/A	N/A	N/A	N/A
PRC-010-0	R2. (Retired)	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).	The responsible entity provided documentation of its current UVLS program assessment more than 30 calendar but less than or equal to 40 calendar days following a request from its Regional Reliability Organization or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 40 calendar days but less than or equal to 50 calendar days following a request from its Regional Reliability Organization or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 50 calendar days but less than or equal to 60 calendar days following a request from its Regional Reliability Organization or NERC.	The responsible entity did not provide documentation of its current UVLS program assessment for more than 60 calendar days following a request from its Regional Reliability Organization or NERC.
PRC-011-0	R1.	The Transmission Owner and Distribution Provider that owns a UVLS system shall have a UVLS equipment maintenance and testing program in place. This program shall include:	The responsible entity's UVLS equipment maintenance and testing program did not address one of the subrequirements in R1.2 through R1.6. OR The responsible entity's UVLS program did not address one of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's UVLS equipment maintenance and testing program did not address two of the subrequirements in R1.2 through R1.6. OR The responsible entity's UVLS program did not address two of the equipment classes as specified in R1.1.1	The responsible entity's UVLS equipment maintenance and testing program did not address three of the subrequirements in R1.1 through R1.6. OR The responsible entity's UVLS program did not address three of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's UVLS equipment maintenance and testing program did not address four or more of the subrequirements in R1.2 through R1.6. OR The responsible entity's UVLS program did not address any of the equipment classes as specified in R1.1.1

Formatted: Font color: Red

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				through R1.1.4.		through R1.1.4.
PRC-011-0	R1.1.	The UVLS system identification which shall include but is not limited to:	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.1.	Relays.	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.2.	Instrument transformers.	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.3.	Communications systems, where appropriate.	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.4.	Batteries.	N/A	N/A	N/A	N/A
PRC-011-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	N/A	N/A	N/A	N/A
PRC-011-0	R1.3.	Summary of testing procedure.	N/A	N/A	N/A	N/A
PRC-011-0	R1.4.	Schedule for system testing.	N/A	N/A	N/A	N/A
PRC-011-0	R1.5.	Schedule for system maintenance.	N/A	N/A	N/A	N/A
PRC-011-0	R1.6.	Date last tested/maintained.	N/A	N/A	N/A	N/A
PRC-011-0	R2.	The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was missing	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was missing for more than 10% up to (and including) 15% of the applicable devices.	The responsible entity did not provide documentation of its UVLS equipment maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was missing for more than 15% of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			for 5% or less of the applicable devices.	missing for more than 5% up to (and including) 10% of the applicable devices.		the applicable devices.
PRC-015-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall maintain a list of and provide data for existing and proposed SPSs as specified in Reliability Standard PRC-013-0_R 1.	N/A	The responsible entity's list of existing or proposed SPSs did not address one of the subrequirements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.	The responsible entity's list of existing or proposed SPSs did not address two of the subrequirements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.	The responsible entity's list of existing or proposed SPSs did not address any of the subrequirements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.
PRC-015-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have evidence it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures as defined in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address one of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address two of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address three of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address four or more of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.
PRC-015-0	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and	The responsible entity provided documentation of its	The responsible entity provided documentation of its	The responsible entity provided documentation of its SPS data and the	The responsible entity provided documentation of its

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).	SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 30 calendar days but less than or equal to 40 calendar days following a request from its Regional Reliability Organization or NERC.	SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 40 calendar days but less than or equal to 50 calendar days following a request from its Regional Reliability Organization or NERC.	results of the studies that show compliance of new or functionally modified SPSs more than 50 calendar days but less than or equal to 60 calendar days following a request from its Regional Reliability Organization or NERC.	SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 60 calendar days following a request from its Regional Reliability Organization or NERC.
PRC-016-0.1	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall analyze its SPS operations and maintain a record of all misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R 1.	N/A	N/A	N/A	The responsible entity that owns an SPS did not analyze its SPS operations and maintain a record of all Misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R 1.
PRC-016-0.1	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall take corrective actions to avoid future misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take 5% or less of the corrective actions designed to avoid future SPS Misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take more than 5% up to (and including) 10% of the corrective actions designed to avoid future SPS Misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take more than 10% up to (and including) 15% of the corrective actions designed to avoid future SPS Misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take more than 15% of the corrective actions designed to avoid future SPS Misoperations.
PRC-016-	R3.	The Transmission Owner, Generator Owner,	The responsible entity	The responsible	The responsible entity	The responsible entity

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
0.1		and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).	provided documentation of its SPS Misoperation analyses and the corrective action plans more than 90 calendar days but less than or equal to 120 calendar days following a request from its Regional Reliability Organization or NERC.	entity provided documentation of its SPS Misoperation analyses and the corrective action plans more than 120 calendar days but less than or equal to 130 calendar days following a request from its Regional Reliability Organization or NERC.	provided documentation of its SPS Misoperation analyses and the corrective action plans more than 130 calendar days but less than or equal to140 calendar days following a request from its Regional Reliability Organization or NERC.	provided documentation of its SPS Misoperation analyses and the corrective action plans more than 140 calendar days following a request from its Regional Reliability Organization or NERC. OR Did not provide the documentation.
PRC-017-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have a system maintenance and testing program(s) in place. The program(s) shall include:	The responsible entity's SPS equipment maintenance and testing program did not address one of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address one of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's SPS equipment maintenance and testing program did not address two of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address two of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's SPS equipment maintenance and testing program did not address three of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address three of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's SPS equipment maintenance and testing program did not address four or more of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address any of the equipment classes as specified in R1.1.1 through R1.1.4.
PRC-017-0	R1.1.	SPS identification shall include but is not limited to:	N/A	N/A	N/A	N/A
PRC-017-0	R1.1.1.	Relays.	N/A	N/A	N/A	N/A
PRC-017-0	R1.1.2.	Instrument transformers.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-017-0	R1.1.3.	Communications systems, where appropriate.	N/A	N/A	N/A	N/A
PRC-017-0	R1.1.4.	Batteries.	N/A	N/A	N/A	N/A
PRC-017-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	N/A	N/A	N/A	N/A
PRC-017-0	R1.3.	Summary of testing procedure.	N/A	N/A	N/A	N/A
PRC-017-0	R1.4.	Schedule for system testing.	N/A	N/A	N/A	N/A
PRC-017-0	R1.5.	Schedule for system maintenance.	N/A	N/A	N/A	N/A
PRC-017-0	R1.6.	Date last tested/maintained.	N/A	N/A	N/A	N/A
PRC-017-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its SPS maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its SPS maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-018-1	R1.	Each Transmission Owner and Generator Owner required to install DMEs by its Regional Reliability Organization (reliability standard PRC-002 Requirements 1-3) shall have DMEs installed that meet the following requirements:	N/A	N/A	The installation of DMEs does not include one of the subrequirements in R1.1 and R1.2.	The installation of DMEs does not include any of the subrequirements in R1.1 and R1.2.
PRC-018-1	R1.1.	Internal Clocks in DME devices shall be synchronized to within 2 milliseconds or less of Universal Coordinated Time scale (UTC)	N/A	N/A	N/A	N/A
PRC-018-1	R1.2.	Recorded data from each Disturbance shall be retrievable for ten calendar days.	N/A	N/A	N/A	N/A
PRC-018-1	R2.	The Transmission Owner and Generator Owner shall each install DMEs in	The responsible entity failed to install 5% or	The responsible entity failed to	The responsible entity failed to install more	The responsible entity failed to install more

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		accordance with its Regional Reliability Organization's installation requirements (reliability standard PRC-002 Requirements 1 through 3).	less of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.	install more than 5% up to (and including) 10% of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.	than 10% up to (and including) 15% of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.	than 15% of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.
PRC-018-1	R3.	The Transmission Owner and Generator Owner shall each maintain, and report to its Regional Reliability Organization on request, the following data on the DMEs installed to meet that region's installation requirements (reliability standard PRC-002 Requirements1.1, 2.1 and 3.1):	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for one of the subrequirements in R3.1 through R3.8.	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for two of the subrequirements in R3.1 through R3.8.	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for three of the subrequirements in R3.1 through R3.8.	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for four or more of the subrequirements in R3.1 through R3.8.
PRC-018-1	R3.1.	Type of DME (sequence of event recorder, fault recorder, or dynamic disturbance recorder).	N/A	N/A	N/A	N/A
PRC-018-1	R3.2.	Make and model of equipment.	N/A	N/A	N/A	N/A
PRC-018-1	R3.3.	Installation location.	N/A	N/A	N/A	N/A
PRC-018-1	R3.4.	Operational status.	N/A	N/A	N/A	N/A
PRC-018-1	R3.5.	Date last tested.	N/A	N/A	N/A	N/A
PRC-018-1	R3.6.	Monitored elements, such as transmission circuit, bus section, etc.	N/A	N/A	N/A	N/A
PRC-018-1	R3.7.	Monitored devices, such as circuit breaker, disconnect status, alarms, etc.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-018-1	R3.8.	Monitored electrical quantities, such as voltage, current, etc.	N/A	N/A	N/A	N/A
PRC-018-1	R4.	The Transmission Owner and Generator Owner shall each provide Disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements (reliability standard PRC-002 Requirement 4).	The responsible entity did not provide 5% or less of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity did not provide more than 5% up to (and including) 10% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity did not provide more than 10% up to (and including) 15% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity did not provide more than 15% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.
PRC-018-1	R5.	The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.	5% or less of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.	More than 5% up to (and including) 10% of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.	More than 10% up to (and including) 15% of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.	More than 15% of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.
PRC-018-1	R6.	Each Transmission Owner and Generator Owner that is required by its Regional Reliability Organization to have DMEs shall have a maintenance and testing program for those DMEs that includes:	N/A	N/A	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include one of the elements in R6.1 and 6.2.	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include any of the elements in R6.1 and 6.2.
PRC-018-1	R6.1.	Maintenance and testing intervals and their basis.	The responsible entity's DME maintenance and testing program was	The responsible entity's DME maintenance and testing program was	The responsible entity's DME maintenance and testing program was non-compliant in that	The responsible entity's DME maintenance and testing program was

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the DME equipment.	non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the DME equipment.	documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the DME equipment.	non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the DME equipment.
PRC-018-1	R6.2.	Summary of maintenance and testing procedures.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for no more than 25% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for more than 25% but less than or equal to 50% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for more than 50% but less than or equal to 75% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for more than 75% of the DME equipment.
PRC-021-1	R1.	Each Transmission Owner and Distribution Provider that owns a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall annually update its UVLS data to support the Regional UVLS program database. The following data shall be provided to the Regional Reliability Organization for each installed UVLS system:	UVLS data was provided but did not address one of the subrequirements in R1.1 through R1.5.	UVLS data was provided but did not address two of the subrequirements in R1.1 through R1.5.	UVLS data was provided but did not address three of the subrequirements in R1.1 through R1.5.	No annual UVLS data was provided. OR UVLS data was provided but did not address four or more of the subrequirements in R1.1 through R1.5.
PRC-021-1	R1.1.	Size and location of customer load, or percent of connected load, to be interrupted.	N/A	N/A	N/A	N/A
PRC-021-1	R1.2.	Corresponding voltage set points and overall	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		scheme clearing times.				
PRC-021-1	R1.3.	Time delay from initiation to trip signal.	N/A	N/A	N/A	N/A
PRC-021-1	R1.4.	Breaker operating times.	N/A	N/A	N/A	N/A
PRC-021-1	R1.5.	Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	N/A	N/A	N/A	N/A
PRC-021-1	R2.	Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.	The responsible entity updated its UVLS data more than 30 calendar days but less than or equal to 40 calendar days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 40 calendar days but less than or equal to 50 calendar days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 50 calendar days but less than or equal to 60 calendar days following a request from its Regional Reliability Organization.	The responsible entity did not update its UVLS data for more than 60 calendar days following a request from its Regional Reliability Organization.
PRC-022-1	R1.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:	The overall analysis program did not address one of the subrequirements in R1.1 through R1.5.	The overall analysis program did not address two of the subrequirements in R1.1 through R1.5.	The overall analysis program did not address three of the subrequirements in R1.1 through R1.5.	The responsible entity failed to analyze and document a UVLS operation and Misoperation. OR The overall analysis program did not address four or more of the subrequirements in R1.1 through R1.5.
PRC-022-1	R1.1.	A description of the event including initiating conditions.	N/A	N/A	N/A	N/A
PRC-022-1	R1.2.	A review of the UVLS set points and tripping times.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-022-1	R1.3.	A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.	N/A	N/A	N/A	N/A
PRC-022-1	R1.4.	A summary of the findings.	N/A	N/A	N/A	N/A
PRC-022-1	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.	N/A	N/A	N/A	N/A
PRC-022-1	R2. (Retired)	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.	The responsible entity provided documentation of the analysis of UVLS program performance more than 90 calendar days but less than or equal to 120 calendar days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 120 calendar days but less than or equal to 130 calendar days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 130 calendar days but less than or equal to 140 calendar days following a request from its Regional Reliability Organization.	The responsible entity did not provide documentation of the analysis of UVLS program performance for more than 140 calendar days following a request from its Regional Reliability Organization.
PRC-023-1	R1.	Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (R1.1 through R1.13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the Bulk Electric System for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees: [Mitigation Time Horizon: Long		Evidence that relay settings comply with criteria in R1.1 though 1.13 exists, but evidence is incomplete or incorrect for one or more of the subrequirements.		Relay settings do not comply with any of the sub requirements R1.1 through R1.13 OR Evidence does not exist to support that relay settings comply with one of the criteria in subrequirements R1.1 through R1.13.

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Term Planning].				
PRC-023-1	R2.	The Transmission Owner, Generator Owner, or Distribution Provider that uses a circuit capability with the practical limitations described in R1.6, R1.7, R1.8, R1.9, R1.12, or R1.13 shall use the calculated circuit capability as the Facility Rating of the circuit and shall obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability. [Time Horizon: Long Term Planning]	Criteria described in R1.6, R1.7. R1.8. R1.9, R1.12, or R.13 was used but evidence does not exist that agreement was obtained in accordance with R2.			
PRC-023-1	R3.	The Planning Coordinator shall determine which of the facilities (transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV) in its Planning Coordinator Area are critical to the reliability of the Bulk Electric System to identify the facilities from 100 kV to 200 kV that must meet Requirement 1 to prevent potential cascade tripping that may occur when protective relay settings limit transmission loadability. [Time Horizon: Long Term Planning]		Provided the list of facilities critical to the reliability of the Bulk Electric System to the appropriate Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers between 31 days and 45 days after the list was established or updated.	Provided the list of facilities critical to the reliability of the Bulk Electric System to the appropriate Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers between 46 days and 60 days after list was established or updated.	Does not have a process in place to determine facilities that are critical to the reliability of the Bulk Electric System. OR Does not maintain a current list of facilities critical to the reliability of the Bulk Electric System, OR Did not provide the list of facilities critical to the reliability of the Bulk Electric System to the appropriate Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers, or provided the list more than 60

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						days after the list was established or updated.
PRC-023-2	R1	Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (Requirement R1, criteria 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees. [See Standard for Criteria]	N/A	N/A	N/A	The responsible entity did not use any one of the following criteria (Requirement R1 criterion 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the Bulk Electric System for all fault conditions. OR The responsible entity did not evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees.
PRC-023-2	R2	Each Transmission Owner, Generator Owner, and Distribution Provider shall set its out-of-step blocking elements to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1.	N/A	N/A	N/A	The responsible entity failed to ensure that its out-of-step blocking elements allowed tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1.

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-023-2	R3	Each Transmission Owner, Generator Owner, and Distribution Provider that uses a circuit capability with the practical limitations described in Requirement R1, criterion 6, 7, 8, 9, 12, or 13 shall use the calculated circuit capability as the Facility Rating of the circuit and shall obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability.	N/A	N/A	N/A	The responsible entity that uses a circuit capability with the practical limitations described in Requirement R1 criterion 6, 7, 8, 9, 12, or 13 did not use the calculated circuit capability as the Facility Rating of the circuit. OR The responsible entity did not obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability.
PRC-023-2	R4	Each Transmission Owner, Generator Owner, and Distribution Provider that chooses to use Requirement R1 criterion 2 as the basis for verifying transmission line relay loadability shall provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays at least once each calendar year, with no more than 15 months between reports.	N/A	N/A	N/A	The responsible entity did not provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits that have transmission line relays set according to the criteria established in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1 criterion 2 at least once each calendar year, with no more than 15 months between reports.
PRC-023-2	R5	Each Transmission Owner, Generator Owner, and Distribution Provider that sets transmission line relays according to Requirement R1 criterion 12 shall provide an updated list of the circuits associated with those relays to its Regional Entity at least once each calendar year, with no more than 15 months between reports, to allow the ERO to compile a list of all circuits that have protective relay settings that limit circuit capability.	N/A	N/A	N/A	The responsible entity did not provide its Regional Entity, with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 12 at least once each calendar year, with no more than 15 months between reports.
PRC-023-2	R6	Each Planning Coordinator shall conduct an assessment at least once each calendar year, with no more than 15 months between assessments, by applying the criteria in Attachment B to determine the circuits in its Planning Coordinator area for which Transmission Owners, Generator Owners, and Distribution Providers must comply with Requirements R1 through R5. The Planning Coordinator shall: *[See standard for what the Planning Coordinator shall do]*	N/A	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but more than 15 months and less than 24 months lapsed between	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but 24 months or more lapsed between assessments. OR The Planning	The Planning Coordinator failed to use the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard. OR The Planning Coordinator used the criteria established

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but failed to include the calendar year in which any criterion in Attachment B first applies. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the	Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 46 days and 60 days after list was established or updated. (part 6.2)	within Attachment B, at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to meet parts 6.1 and 6.2. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to maintain the list of circuits determined according to the process described in Requirement R6. (part 6.1)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 31 days and 45 days after the list was established or updated. (part 6.2)		OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 but failed to provide the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area or provided the list more than 60 days after the list was established or updated. (part 6.2) OR The Planning Coordinator failed to determine the circuits in its Planning Coordinator area for

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						which applicable entities must comply with the standard.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-001-1a	R1.	Each Transmission Operator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area and shall exercise specific authority to alleviate operating emergencies.	N/A	N/A	N/A	The Transmission Operator has no evidence that clear decision-making authority exists to assure reliability in its area or has failed to exercise this authority to alleviate operating emergencies.
TOP-001-1a	R2.	Each Transmission Operator shall take immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.	N/A	N/A	N/A	The Transmission Operator failed to have evidence that it took immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.
TOP-001-1a	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the	N/A	N/A	N/A	The responsible entity failed to comply with reliability directives issued by the Reliability Coordinator or the Transmission Operator (when applicable), when said directives would not have resulted in actions that would violate safety,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.				equipment, regulatory or statutory requirements, or under circumstances that said directives would have resulted in actions that would violate safety, equipment, regulatory or statutory requirements the responsible entity failed to inform the Reliability Coordinator or Transmission Operator (when applicable) of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator could implement alternate remedial actions.
TOP-001-1a	R4.	Each Distribution Provider and Load-Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions.	N/A	N/A	N/A	The responsible entity failed to comply with all reliability directives issued by the Transmission Operator, including shedding firm load, when said directives would not have resulted in actions that would violate safety, equipment, regulatory or statutory requirements, or under

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						circumstances when said directives would have violated safety, equipment, regulatory or statutory requirements, the responsible entity failed to immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator could implement alternate remedial actions.
TOP-001-1a	R5.	Each Transmission Operator shall inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, and take actions to avoid, when possible, or mitigate the emergency.	N/A	The Transmission Operator failed to inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, but did take actions to avoid, when possible, or mitigate the emergency.	N/A	The Transmission Operator failed to inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, and failed to take actions to avoid, when possible, or mitigate the emergency.
TOP-001-1a	R6.	Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.	N/A	N/A	N/A	The responsible entity failed to render all available emergency assistance to others as requested, after the requesting entity had implemented its comparable

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						emergency procedures, when said assistance would not have resulted in actions that would violate safety, equipment, or regulatory or statutory requirements.
TOP-001-1a	R7.	Each Transmission Operator and Generator Operator shall not remove Bulk Electric System facilities from service if removing those facilities would burden neighboring systems unless:	N/A	N/A	N/A	The responsible entity removed Bulk Electric System facilities from service and removal of said facilities burdened a neighboring system, without complying with the applicable requirements listed in R7.1 through R7.3.
TOP-001-1a	R7.1.	For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	N/A
TOP-001-1a	R7.2.	For a transmission facility, the Transmission Operator shall notify and coordinate with its Reliability Coordinator. The Transmission Operator shall notify other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	N/A
TOP-001-1a	R7.3.	When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public,	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.				
TOP-001-1a	R8.	During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.	N/A	N/A	N/A	The responsible entity failed to take immediate actions to restore the Real and Reactive Power Balance during a system emergency. OR The responsible entity failed to request emergency assistance from the Reliability Coordinator during a period when it was unable to restore the Real and Reactive Power Balance, OR During a period when corrective actions or emergency assistance was not adequate to mitigate the Real and Reactive Power Balance, the responsible entity failed to implement firm load shedding.
TOP-002-2.1b	R1.	Each Balancing Authority and Transmission Operator shall maintain a set of current plans	N/A	N/A	The responsible entity maintained a set of	The responsible entity failed to maintain a set

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that are designed to evaluate options and set procedures for reliable operation through a reasonable future time period. In addition, each Balancing Authority and Transmission Operator shall be responsible for using available personnel and system equipment to implement these plans to ensure that interconnected system reliability will be maintained.			current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period, but failed to utilize available personnel and system equipment to implement these plans to ensure that interconnected system reliability would be maintained.	of current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period.
TOP-002-2.1b	R2.	Each Balancing Authority and Transmission Operator shall ensure its operating personnel participate in the system planning and design study processes, so that these studies contain the operating personnel perspective and system operating personnel are aware of the planning purpose.	N/A	N/A	N/A	The responsible entity failed to ensure its operating personnel participated in the system planning and design study processes.
TOP-002-2.1b	R3.	Each Load-Serving Entity and Generator Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider. Each Balancing Authority and Transmission Service Provider shall coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed to coordinate its seasonal	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				operations with its Transmission Operator.		to coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.
TOP-002-2.1b	R4.	Each Balancing Authority and Transmission Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator, so that normal Interconnection operation will proceed in an orderly and consistent manner.	N/A	The responsible entity failed to coordinate (where confidentiality agreements allow) one of the following three categories of operations (current-day, next-day or seasonal) with the applicable entity(ies)	The responsible entity failed to coordinate (where confidentiality agreements allow) two of the following three categories of operations (current-day, next-day or seasonal) with the applicable entity(ies)	The responsible entity failed to coordinate (where confidentiality agreements allow) all three of the following categories of operations (current-day, next-day or seasonal) with the applicable entity(ies)
TOP-002-2.1b	R5.	Each Balancing Authority and Transmission Operator shall plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.	N/A	N/A	N/A	The responsible entity failed to plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.
TOP-002-2.1b	R6.	Each Balancing Authority and Transmission Operator shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional, and local reliability requirements.	N/A	N/A	N/A	The responsible entity failed to plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional and local reliability

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requirements.
TOP-002-2.1b	R7.	Each Balancing Authority shall plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.
TOP-002-2.1b	R8.	Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.
TOP-002-2.1b	R9.	Each Balancing Authority shall plan to meet Interchange Schedules and Ramps.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet Interchange Schedules and Ramps.
TOP-002-2.1b	R10.	Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).	N/A	N/A	N/A	The responsible entity failed to plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).
TOP-002-2.1b	R11.	The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs. Neighboring Transmission Operators shall utilize identical SOLs for common facilities. The Transmission Operator shall update	N/A	N/A	The Transmission Operator performed seasonal, next-day, and current-day Bulk Electric System studies, reflecting	The Transmission Operator failed to perform seasonal, next-day, or current-day Bulk Electric System studies,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject confidentiality requirements), and to its Reliability Coordinator.			current system conditions, to determine SOLs, but failed to make the results of Bulk Electric System studies available to all of the Transmission Operators, Balancing Authorities (subject confidentiality requirements), or to its Reliability Coordinator.	reflecting current system conditions, to determine SOLs.
TOP-002-2.1b	R12.	The Transmission Service Provider shall include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available Transfer Capability calculation processes.	N/A	N/A	N/A	The Transmission Service Provider failed to include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available Transfer Capability calculation processes.
TOP-002-2.1b	R13.	At the request of the Balancing Authority or Transmission Operator, a Generator Operator shall perform generating real and reactive capability verification that shall include, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, and provide the results to the Balancing Authority or Transmission Operator operating personnel as requested.	N/A	N/A	N/A	The Generator Operator failed to perform generating real and reactive capability verification that included, among other variables, weather, ambient air and water conditions,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						and fuel quality and quantity, or failed to provide the results of generating real and reactive verifications Balancing Authority or Transmission Operator operating personnel, when requested.
TOP-002-2.1b	R14.	Generator Operators shall, without any intentional time delay, notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics including but not limited to:	N/A	N/A	N/A	The Generator Operator failed to notify its Balancing Authority or Transmission Operator of changes in capabilities and characteristics including real output capabilities.
TOP-002-2.1b	R14.1.	Changes in real output capabilities.	N/A	N/A	N/A	N/A
TOP-002-2.1b	R15.	Generation Operators shall, at the request of the Balancing Authority or Transmission Operator, provide a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).	N/A	N/A	N/A	The Generator Operator failed to provide, at the request of the Balancing Authority or Transmission Operator, a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).
TOP-002-2.1b	R16.	Subject to standards of conduct and confidentiality agreements, Transmission	N/A	N/A	N/A	The Transmission Operator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators shall, without any intentional time delay, notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics including but not limited to:				notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2.1b	R16.1.	Changes in transmission facility status.	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility status, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2.1b	R16.2.	Changes in transmission facility rating.	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility rating, within the terms and conditions of standards of conduct and confidentiality agreements.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-002-2.1b	R17.	Balancing Authorities and Transmission Operators shall, without any intentional time delay, communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.	N/A	N/A	N/A	The responsible entity failed to communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.
TOP-002-2.1b	R18.	Neighboring Balancing Authorities, Transmission Operators, Generator Operators, Transmission Service Providers, and Load-Serving Entities shall use uniform line identifiers when referring to transmission facilities of an interconnected network.	N/A	N/A	N/A	The responsible entity failed to use uniform line identifiers when referring to transmission facilities of an interconnected network.
TOP-002-2.1b	R19.	Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations.	N/A	N/A	N/A	The responsible entity failed to maintain accurate computer models utilized for analyzing and planning system operations.
TOP-004-2	R1.	Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).	N/A	N/A	N/A	The Transmission Operator failed to operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).
TOP-004-2	R2.	Each Transmission Operator shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.	N/A	N/A	N/A	The Transmission Operator failed to operate so that instability, uncontrolled separation, or cascading outages

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						would not occur as a result of the most severe single contingency.
TOP-004-2	R3.	Each Transmission Operator shall operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by its Reliability Coordinator.	N/A	N/A	N/A	The Transmission Operator failed to operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by Reliability Coordinator policy.
TOP-004-2	R4.	If a Transmission Operator enters an unknown operating state (i.e., any state for which valid operating limits have not been determined), it will be considered to be in an emergency and shall restore operations to respect proven reliable power system limits within 30 minutes.	N/A	N/A	N/A	The Transmission Operator entered an unknown operating state (i.e., any state for which valid operating limits have not been determined), and failed to restore operations to respect proven reliable power system limits for more than 30 minutes.
TOP-004-2	R5.	Each Transmission Operator shall make every effort to remain connected to the Interconnection. If the Transmission Operator determines that by remaining interconnected, it is in imminent danger of violating an IROL or SOL, the Transmission Operator may take such actions, as it deems necessary, to protect its area.	N/A	N/A	N/A	The Transmission Operator did not make every effort to remain connected to the Interconnection except when the Transmission Operator determined that by remaining

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						interconnected, it was in imminent danger of violating an IROL or SOL.
TOP-004-2	R6.	Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including:	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include information required by one of the subrequirements R6.1 thru R6.4	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include information required by 2 of the subrequirements R6.1 thru R6.4.	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include information required by 3 of the subrequirements R6.1 thru R6.4.	The Transmission Operator, failed to develop, maintain, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability. If formal policies and procedures were developed, such policies and procedures failed to include any of the information required in subrequirements R6.1 thru R6.4.
TOP-004-2	R6.1.	Monitoring and controlling voltage levels and real and reactive power flows.	N/A	N/A	N/A	N/A
TOP-004-2	R6.2.	Switching transmission elements.	N/A	N/A	N/A	N/A
TOP-004-2	R6.3.	Planned outages of transmission elements.	N/A	N/A	N/A	N/A
TOP-004-2	R6.4.	Responding to IROL and SOL violations.	N/A	N/A	N/A	N/A
TOP-007-0	R1.	A Transmission Operator shall inform its Reliability Coordinator when an IROL or SOL has been exceeded and the actions being taken to return the system to within	N/A	N/A	The Transmission Operator informed its Reliability Coordinator when an IROL or SOL had been exceeded but	The Transmission Operator failed to inform its Reliability Coordinator when an IROL or SOL had

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		limits.			failed to provide the actions being taken to return the system to within limits.	been exceeded.
TOP-007-0	R2.	Following a Contingency or other event that results in an IROL violation, the Transmission Operator shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes.	Following a Contingency or other event that resulted in an IROL violation of a magnitude of 5% or less, the Transmission Operator failed to return its transmission system to within the IROL in less than or equal to 35 minutes.	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within the IROL in accordance with the following: (a) an IROL with a magnitude of 5% or less for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (b) an IROL with a magnitude of more than 5% up to (and including) 10% for a period of time less than or equal to 40 minutes, or (c) an IROL with a magnitude of more than 10% up to (and including) 15% for a period of time less than or equal to 35 minutes.	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within the IROL in accordance with the following: (a) an IROL with a magnitude of 5% or less for a period of time greater than 45 minutes, or (b) an IROL with a magnitude of more than 5% up to (and including) 10% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude of more than 10% up to (and including) 15% for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (d) an IROL with a magnitude of more than 15% up to (and including) 20% for a	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within the IROL in accordance with the following: (a) an IROL with a magnitude of more than 10% up to (and including) 15% for a period of time greater than 45 minutes, or (b) an IROL with a magnitude of more than 15% up to (and including) 20% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude of more than 20% up to (and including) 25% for a period of time greater than 35 minutes, or (d) an IROL with a magnitude of more than 25% for a period of greater than 30 minutes.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					period of time less than or equal to 40 minutes, or (e) an IROL with a magnitude of more than 20% up to (and including) 25% for a period of time less than or equal to 35 minutes.	
TOP-007-0	R3.	A Transmission Operator shall take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to comply with Requirement R 2.	N/A	N/A	N/A	The Transmission Operator failed to take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to return the transmission system to IROL within 30 minutes.
TOP-007-0	R4.	The Reliability Coordinator shall evaluate actions taken to address an IROL or SOL violation and, if the actions taken are not appropriate or sufficient, direct actions required to return the system to within limits.	N/A	N/A	N/A	The Reliability Coordinator failed to evaluate actions taken to address an IROL or SOL violation and, if the actions taken were not appropriate or sufficient, direct actions required to return the system to within limits.
TOP-008-1	R1.	The Transmission Operator experiencing or contributing to an IROL or SOL violation shall take immediate steps to relieve the condition, which may include shedding firm load.	N/A	N/A	N/A	The Transmission Operator experiencing or contributing to an IROL or SOL violation failed to take immediate steps to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						relieve the condition, which may have included shedding firm load.
TOP-008-1	R2.	Each Transmission Operator shall operate to prevent the likelihood that a disturbance, action, or inaction will result in an IROL or SOL violation in its area or another area of the Interconnection. In instances where there is a difference in derived operating limits, the Transmission Operator shall always operate the Bulk Electric System to the most limiting parameter.	N/A	N/A	The Transmission Operator operated to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection but failed to operate the Bulk Electric System to the most limiting parameter in instances where there was a difference in derived operating limits.	The Transmission Operator failed to operate to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection.
TOP-008-1	R3.	The Transmission Operator shall disconnect the affected facility if the overload on a transmission facility or abnormal voltage or reactive condition persists and equipment is endangered. In doing so, the Transmission Operator shall notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection prior to switching, if time permits, otherwise, immediately thereafter.	N/A	N/A	The Transmission Operator disconnected the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered but failed to notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection either prior to	The Transmission Operator failed to disconnect the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					switching, if time permitted, otherwise, immediately thereafter.	
TOP-008-1	R4.	The Transmission Operator shall have sufficient information and analysis tools to determine the cause(s) of SOL violations. This analysis shall be conducted in all operating timeframes. The Transmission Operator shall use the results of these analyses to immediately mitigate the SOL violation.	N/A	N/A	The Transmission Operator had sufficient information and analysis tools to determine the cause(s) of SOL violations and used the results of these analyses to immediately mitigate the SOL violation(s), but failed to conduct these analyses in all operating timeframes.	The Transmission Operator failed to have sufficient information and analysis tools to determine the cause(s) of SOL violations or failed to use the results of analyses to immediately mitigate the SOL violation.

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-001-0.1	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I. To be considered valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-001-0.1	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-001-0.1	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category A of Table 1 (no contingencies). The specific elements selected (from each of the following categories) shall be acceptable to the associated Regional Reliability	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Organization(s).				
TPL-001-0.1	R1.3.1.	Cover critical system conditions and study years as deemed appropriate by the entity performing the study.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-001-0.1	R1.3.2.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system testing) AND most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.
TPL-001-0.1	R1.3.3.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system simulation testing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						show marginal conditions that may require longer lead-time solutions.
TPL-001-0.1	R1.3.4.	Have established normal (pre-contingency) operating procedures in place.	N/A	N/A	N/A	No precontingency operating procedures are in place for existing facilities.
TPL-001-0.1	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-001-0.1	R1.3.6.	Be performed for selected demand levels over the range of forecast system demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-001-0.1	R1.3.7.	Demonstrate that system performance meets Table 1 for Category A (no contingencies).	N/A	N/A	N/A	No past or current study results exist showing pre-contingency system analysis.
TPL-001-0.1	R1.3.8.	Include existing and planned facilities.	The responsible entity’s transmission model used for past or current studies and/or	The responsible entity’s transmission model used for past or current studies and/or	N/A	The responsible entity's transmission model used for past or current studies and/or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.		system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-001-0.1	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-001-0.1	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category A.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category A planning requirements.
TPL-001-0.1	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-001-0_R1, the Planning Authority and Transmission Planner shall each:	N/A	The responsible entity has failed to review the continuing need for previously identified facility additions through subsequent annual assessments. (R2.2)	The responsible entity provided documented evidence of corrective action plans in order to satisfy Category A planning requirements, but failed to include an implementation schedule with in-service dates (R2.1.1 and R2.1.2) OR The responsible entity	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category A planning requirements. (R2.1)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					failed to consider necessary lead times to implement its corrective action plan. (R2.1.3)	
TPL-001-0.1	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	N/A	N/A	N/A	N/A
TPL-001-0.1	R3.	The Planning Authority and Transmission Planner shall each document the results of these reliability assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-002-0b	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:	25% or less of the sub-components.	more than 25% but less than 50% of the sub-components.	50% or more but less than 75% of the sub-components.	75% or more of the sub-components.
TPL-002-0b	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-002-0b	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-002-0b	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-002-0b	R1.3.1.	Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies	N/A	The responsible entity provided evidence through current or past studies and/or	N/A	The responsible entity did not provided evidence through current or past studies

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.		system simulation testing that selected NERC Category B contingencies were evaluated, however, no rational was provided to indicate why the remaining Category B contingencies for their system were not evaluated.		and/or system simulation testing to indicate that any NERC Category B contingencies were evaluated.
TPL-002-0b	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-002-0b	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies (and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are no longer valid.
TPL-002-0b	R1.3.4.	Be conducted beyond the five-year horizon	N/A	N/A	N/A	The responsible entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		only as needed to address identified marginal conditions that may have longer lead-time solutions.				failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system simulation testing show marginal conditions that may require longer lead-time solutions.
TPL-002-0b	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-002-0b	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system Demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-002-0b	R1.3.7.	Demonstrate that system performance meets Category B contingencies.	N/A	N/A	N/A	No past or current study results exist showing Category B

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						contingency system analysis.
TPL-002-0b	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-002-0b	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-002-0b	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-002-0b	R1.3.11.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect	The responsible entity's transmission model used for past or current studies is deficient with respect

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					to the effects of planned control devices.	to the effects of existing control devices.
TPL-002-0b	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-002-0b	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category B of Table I.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category B planning requirements.
TPL-002-0b	R1.5.	Consider all contingencies applicable to Category B.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to 25% or less of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient 75% or more of all applicable contingencies.
TPL-002-0b	R2.	When System simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-002-0_R1, the Planning Authority and Transmission Planner shall each:	N/A	The responsible entity has failed to review the continuing need for previously identified facility	The responsible entity provided documented evidence of corrective action plans in order to satisfy Category B	The responsible entity has failed to provide documented evidence of corrective action plans in order to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				additions through subsequent annual assessments. (R2.2)	planning requirements, but failed to include a implementation schedule with in-service dates (R2.1.1 and R2.1.2) OR The responsible entity failed to consider necessary lead times to implement its corrective action plan. (R2.1.3)	satisfy Category B planning requirements. (R2.1)
TPL-002-0b	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	N/A
TPL-002-0b	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	N/A
TPL-002-0b	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	N/A
TPL-002-0b	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	N/A
TPL-002-0b	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	N/A	N/A	N/A	N/A
TPL-002-0b	R3.	The Planning Authority and Transmission Planner shall each document the results of its Reliability Assessments and corrective plans and shall annually provide the results to its respective Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Regional Reliability Organization(s) as required by the Regional Reliability Organization.		respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.
TPL-003-0a	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-003-0a	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-003-0a	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-003-0a	R1.3.	Be supported by a current or past study and/or system simulation testing that	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	25% or less of the sub-components.	more than 25% but less than 50% of the sub-components.	50% or more but less than 75% of the sub-components.	75% or more of the sub-components.
TPL-003-0a	R1.3.1.	Be performed and evaluated only for those Category C contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.	N/A	The responsible entity provided evidence through current or past studies that selected NERC Category C contingencies were evaluated, however, no rational was provided to indicate why the remaining Category C contingencies for their system were not evaluated.	N/A	The responsible entity did not provided evidence through current or past studies to indicate that any NERC Category C contingencies were evaluated.
TPL-003-0a	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-003-0a	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.		(and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are no longer valid.
TPL-003-0a	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system testing show marginal conditions that may require longer lead-time solutions.
TPL-003-0a	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-003-0a	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast	N/A	N/A	N/A	The responsible entity has failed to produce

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system demands.				evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-003-0a	R1.3.7.	Demonstrate that System performance meets Table 1 for Category C contingencies.	N/A	N/A	N/A	No past or current study results exists showing Category C contingency system analysis.
TPL-003-0a	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-003-0a	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet System performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-003-0a	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is	The responsible entity's transmission model used for past or current studies is

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-003-0a	R1.3.11.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.
TPL-003-0a	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those Demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-003-0a	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category C.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category C planning requirements.
TPL-003-0a	R1.5.	Consider all contingencies applicable to Category C.	The responsible entity has considered the NERC Category C contingencies applicable to their	The responsible entity has considered the NERC Category C contingencies applicable to their	The responsible entity has considered the NERC Category C contingencies applicable to their	The responsible entity has considered the NERC Category C contingencies applicable to their

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			system, but was deficient with respect to 25% or less of all applicable contingencies.	system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	system, but was deficient 75% or more of all applicable contingencies.
TPL-003-0a	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-003-0_R1, the Planning Authority and Transmission Planner shall each:	N/A	The responsible entity has failed to review the continuing need for previously identified facility additions through subsequent annual assessments. (R2.2)	The responsible entity provided documented evidence of corrective action plans in order to satisfy Category C planning requirements, but failed to include an implementation schedule with in-service dates. (R2.1.1 and R2.1.2) OR The responsible entity failed to consider necessary lead times to implement its corrective action plan. (R2.1.3)	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category C planning requirements. (R2.1)
TPL-003-0a	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	N/A
TPL-003-0a	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	N/A
TPL-003-0a	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	N/A
TPL-003-0a	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	N/A
TPL-003-0a	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		continuing need for identified system facilities. Detailed implementation plans are not needed.				
TPL-003-0a	R3.	The Planning Authority and Transmission Planner shall each document the results of these Reliability Assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.
TPL-004-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Table I. To be valid, the Planning Authority's and Transmission Planner's assessment shall:	The responsible entity is non-compliant with one of the sub-components of requirement R1.3 (R1.3.1 through R1.3.9). OR The responsible entity has considered the NERC Category D contingencies applicable to their system, but was deficient with respect to 5% or less of all applicable contingencies. (R1.4)	The responsible entity is non-compliant with two of the sub-components of requirement R1.3 (R1.3.1 through 1.3.9). OR The responsible entity has considered the NERC Category D contingencies applicable to their system, but was deficient with respect to more than 5% up to (and including) 10% of all applicable contingencies. (R1.4)	The responsible entity is non-compliant with three of the sub-components of requirement R1.3 (R1.3.1 through 1.3.9). OR The responsible entity has considered the NERC Category D contingencies applicable to their system, but was deficient with respect to more than 10% up to (and including) 15% of all applicable contingencies. (R1.4)	The responsible entity did not perform the transmission assessments annually. (R1.1) OR The responsible entity has failed to demonstrate a valid assessment for the near-term planning period. (R1.2) OR The responsible entity is non-compliant with four or more of the sub-components of requirement R1.3 (R1.3.1 through 1.3.9).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The responsible entity has considered the NERC Category D contingencies applicable to its system, but was deficient with respect to more than 15% of all applicable contingencies. (R1.4)
TPL-004-0	R1.1.	Be made annually.	N/A	N/A	N/A	N/A
TPL-004-0	R1.2.	Be conducted for near-term (years one through five).	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category D contingencies of Table I. The specific elements selected (from within each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.1.	Be performed and evaluated only for those Category D contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-004-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.4.	Have all projected firm transfers modeled.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.5.	Include existing and planned facilities.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.6.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.7.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.8.	Include the effects of existing and planned control devices.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.9.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	N/A
TPL-004-0	R1.4.	Consider all contingencies applicable to Category D.	N/A	N/A	N/A	N/A
TPL-004-0	R2.	The Planning Authority and Transmission Planner shall each document the results of its reliability assessments and shall annually provide the results to its entities' respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.	N/A	The responsible entity DID NOT document the results of its annual reliability assessments AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-001-2	R1.	Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 5% or less of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting between 5-10% of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 10-15%, inclusive, of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting greater than 15% of their individual and neighboring areas voltage levels and Mvar flows.
VAR-001-2	R2.	Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 95% but less than 100% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 90% but less than 95% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 85% but less than 90% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired less than 85% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.
VAR-001-2	R3.	The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.	N/A	N/A	N/A	The Transmission Operator did not specify criteria that exempts generators from compliance with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the requirements defined in Requirement 4, and Requirement 6.1. to all of the parties involved.
VAR-001-2	R3.1.	Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing one or more entities. The missing entities shall represent less than 25% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing two or more entities. The missing entities shall represent less than 50% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing three or more entities. The missing entities shall represent less than 75% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing four or more entities. The missing entities shall represent 75% or more of those eligible for the list.
VAR-001-2	R3.2.	For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.	The Transmission Operator failed to notify up to 25% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 25% up to 50% of the associated Generator Owners of each generator that are on this exemption list.	The Transmission Operator failed to notify 50% up to 75% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 75% up to 100% of the associated Generator Owner of each generator that are on this exemption list.
VAR-001-2	R4.	Each Transmission Operator shall specify a voltage or Reactive Power schedule [4] at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the	N/A	N/A	The Transmission Operator provide Voltage or Reactive Power schedules were for some but not all generating units as required in R4.	The Transmission Operator provide No evidence that voltage or Reactive Power schedules were provided to Generator Operators as required

[4] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).				in R4.
VAR-001-2	R5. (Retired)	Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 5% or less of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting between 5-10% of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 10-15%, inclusive, of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting greater than 15% of its reactive requirements.
VAR-001-2	R6.	The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting 5% or less of the required resources.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting between 5-10% of the required resources.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting 10-15%, inclusive, of the required resources.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting 15% or greater of required resources.
VAR-001-2	R6.1.	When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.	N/A	N/A	N/A	The Transmission Operator has not provided evidence to show that directives were issued to the Generator Operator to maintain or change either its voltage schedule or its Reactive Power

Formatted: Font color: Red

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						schedule in accordance with R6.1.
VAR-001-2	R7.	The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 5% or less of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting between 5-10% of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 10-15%, inclusive, of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting greater than 15% of the required devices.
VAR-001-2	R8.	Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 5% or less of the required resources.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting between 5-10% of the required resources.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 10-15%, inclusive, of the required resources.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting greater than 15% of the required resources.
VAR-001-2	R9.	Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to support its voltage under first Contingency conditions.	The Transmission Operator maintains 95% or more of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 85% or more but less than 95% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 75% or more but less then 85% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains less than 75% of the reactive resources needed to support its voltage under first Contingency conditions.
VAR-001-2	R9.1.	Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.	The applicable entity did not disperse and/or locate the reactive resources, as directed in	The applicable entity did not disperse and/or locate the reactive resources, as	The applicable entity did not disperse and/or locate the reactive resources, as directed	The applicable entity did not disperse and/or locate the reactive resources, as directed

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the requirement, affecting 5% or less of the resources.	directed in the requirement, affecting between 5-10% of the resources.	in the requirement, affecting 10-15%, inclusive, of the resources.	in the requirement, affecting greater than 15% of the resources.
VAR-001-2	R10.	Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 5% or less of the violations.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting between 5-10% of the violations.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 10-15%, inclusive, of the violations.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting greater than 15% of the violations.
VAR-001-2	R11.	After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes and a timeframe for making these changes, but failed to provide technical justification for these changes.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes, but failed to provide a timeframe for making these changes and technical justification for these changes.	The Transmission Operator failed to provide documentation to the Generator Owner specifying required step-up transformer tap changes, a timeframe for making these changes, and technical justification for these changes.	N/A
VAR-001-2	R12.	The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.	N/A	N/A	N/A	The Transmission Operator has failed to direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1b	R1.	The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator.	N/A	N/A	N/A	The responsible entity did not operate each generator in the automatic voltage control mode and failed to notify the Transmission Operator as identified in R1.
VAR-002-1.1b	R2.	Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings. [1] as directed by the Transmission Operator	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by 5% or less.	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by more than 5% up to (and including) 10% OR When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by more than 10% up to (and including) 15%	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by more than 15%. OR When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Reactive Power schedule directed by the Transmission Operator. OR The Generator Operator failed to provide an explanation of why the voltage schedule could not be met.		directed by the Transmission Operator and the Generator Operator failed to provide an explanation of why the voltage schedule could not be met.
VAR-002-1.1b	R2.1.	When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R2.2.	When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R3.	Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:	N/A	N/A	The Generator Operator failed to notify the Transmission Operator within 30 minutes of the information as specified in either R3.1 or R3.2	The Generator Operator failed to notify the Transmission Operator within 30 minutes of the information as specified in both R3.1 and R3.2
VAR-002-1.1b	R3.1.	A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1b	R3.2.	A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.	The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner one of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 30, but less than or equal to 35 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner two of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 35, but less than or equal to 40 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner three of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 40, but less than or equal to 45 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner any of the types of data as specified in R4.1.1 and R 4.1.2 and 4.1.3 and 4.1.4 OR The information was provided in more than 45 calendar days of the request.
VAR-002-1.1b	R4.1.	For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.1.	Tap settings.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.2.	Available fixed tap ranges.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.3.	Impedance data.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.4.	The +/- voltage range with step-change in % for load-tap changing transformers.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1b	R5.	After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.	N/A	N/A	N/A	The responsible entity failed to ensure that transformer tap positions were changed according to the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.
VAR-002-1.1b	R5.1.	If the Generator Operator can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.	N/A	N/A	N/A	The responsible entity failed to notify the Transmission Operator and to provide technical justification.
VAR-002-WECC-1	R1.	Generator Operators and Transmission Operators shall have AVR in service and in automatic voltage control mode 98% of all operating hours for synchronous generators or synchronous condensers. Generator Operators and Transmission Operators may exclude hours for R1.1 through R1.10 to achieve the 98% requirement. [*See Standard pdf for R1.1 through R1.10*]	AVR is in service less than 98% but at least 90% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.	AVR is in service less than 90% but at least 80% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.	AVR is in service less than 80% but at least 70% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.	AVR is in service less than 70% of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.
VAR-002-WECC-1	R2.	Generator Operators and Transmission Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.10.	There shall be a Lower Level of non-compliance if documentation is incomplete with any requirement R1.1	There shall be a Moderate Level of non-compliance if the Generator Operator does not have documentation to	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			through R1.10.	demonstrate compliance with any requirement R1.1 through R1.10.		
VAR-501-WECC-1	R1.	Generator Operators shall have PSS in service 98% of all operating hours for synchronous generators equipped with PSS. Generator Operators may exclude hours for R1.1 through R1.12 to achieve the 98% requirement. [*See Standard pdf for R1.1 through R1.12*]	PSS is in service less than 98% but at least 90% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.	PSS is in service less than 90% but at least 80% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.	PSS is in service less than 80% but at least 70% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.	PSS is in service less than 70% of all hours during which the synchronous generating unit is on line for each calendar quarter.
VAR-501-WECC-1	R2.	Generator Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.12.	There shall be a Lower Level of non-compliance if documentation is incomplete with any requirement R1.1 through R1.12.	There shall be a Moderate Level of non-compliance if the Generator Operator does not have documentation to demonstrate compliance with any requirement R1.1 through R1.12.	N/A	N/A

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

NERC Reliability Standards VSL Change History Table:

Date	Standard	Requirement	Action
9/25/12	BAL-005-0.2b, EOP-001-0.1b, EOP-002-3.1, PER-001-0.2 & TOP-002-2.1b		FERC approved Errata - Added
TBD	BAL-005-0.2b, CIP-001-2a, CIP-003-3, CIP-003-4, CIP-005-3a, CIP-005-4a, CIP-007-3, CIP-007-4, EOP-004-1, FAC-002-1, FAC-008-1, FAC-008-3, FAC-010-2.1, FAC-011-2, FAC-013-2, INT-007-1, IRO-016-1, NUC-001-2, PRC-010-0, PRC-022-1, VAR-001-2		Various VSLs retired as part of the Paragraph 81 project (Project 2013-02)

Standard Version	Requirement Name	Status	Requirement Text
BAL-005-0.2b	R2.	Kept in Final SAR for Retirement	Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.
CIP-001-2a	R4.	Kept in Final SAR for Retirement	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.
CIP-003-3	R1.2.	Kept in Final SAR for Retirement	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-3	R3.	Kept in Final SAR for Retirement	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
CIP-003-3	R3.1.	Kept in Final SAR for Retirement	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
CIP-003-3	R3.2.	Kept in Final SAR for Retirement	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
CIP-003-3	R3.3.	Kept in Final SAR for Retirement	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
CIP-003-3	R4.2.	Kept in Final SAR for Retirement	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	R1.2.	Kept in Final SAR for Retirement	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-4	R3.	Kept in Final SAR for Retirement	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
CIP-003-4	R3.1.	Kept in Final SAR for Retirement	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
CIP-003-4	R3.2.	Kept in Final SAR for Retirement	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
CIP-003-4	R3.3.	Kept in Final SAR for Retirement	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
CIP-003-4	R4.2.	Kept in Final SAR for Retirement	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Standard Version	Requirement Name	Status	Requirement Text
CIP-005-3a	R2.6.	Kept in Final SAR for Retirement	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
CIP-005-4a	R2.6.	Kept in Final SAR for Retirement	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
CIP-007-3	R7.3.	Kept in Final SAR for Retirement	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
CIP-007-4	R7.3.	Kept in Final SAR for Retirement	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
COM-001-1.1	R6.	Kept in Final SAR for Information Only	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001, "NERCNet Security Policy."
EOP-004-1	R1.	Kept in Final SAR for Retirement	Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.
EOP-005-2	R3.1.	Kept in Final SAR for Retirement	If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.
EOP-009-0	R2.	Kept in Final SAR for Information Only	The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.
FAC-002-1	R2.	Kept in Final SAR for Retirement	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).
FAC-008-1	R1.3.5.	Kept in Final SAR for Information Only	Other assumptions.
FAC-008-1	R2.	Kept in Final SAR for Retirement	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

Standard Version	Requirement Name	Status	Requirement Text
FAC-008-1	R3.	Kept in Final SAR for Retirement	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.
FAC-008-3	R4.	Kept in Final SAR for Retirement	Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.
FAC-008-3	R5.	Kept in Final SAR for Retirement	If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.
FAC-010-2.1	R5.	Added to Final SAR for Retirement	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.
FAC-011-2	R5.	Added to Final SAR for Retirement	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Standard Version	Requirement Name	Status	Requirement Text
FAC-013-2	R3.	Kept in Final SAR for Retirement	If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.
INT-007-1	R1.2.	Kept in Final SAR for Retirement	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.
IRO-016-1	R2.	Kept in Final SAR for Retirement	The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.
MOD-004-1	R1.	Deferred to Subsequent Phase	The Transmission Service Provider that maintains CBM shall prepare and keep current a "Capacity Benefit Margin Implementation Document" (CBMID) that includes, at a minimum, the following information:
MOD-004-1	R1.1.	Deferred to Subsequent Phase	The process through which a Load-Serving Entity within a Balancing Authority Area associated with the Transmission Service Provider, or the Resource Planner associated with that Balancing Authority Area, may ensure that its need for Transmission capacity to be set aside as CBM will be reviewed and accommodated by the Transmission Service Provider to the extent Transmission capacity is available.
MOD-004-1	R1.2.	Deferred to Subsequent Phase	The procedure and assumptions for establishing CBM for each Available Transfer Capability (ATC) Path or Flowgate.
MOD-004-1	R1.3.	Deferred to Subsequent Phase	The procedure for a Load-Serving Entity or Balancing Authority to use Transmission capacity set aside as CBM, including the manner in which the Transmission Service Provider will manage situations where the requested use of CBM exceeds the amount of CBM available.
MOD-004-1	R2.	Deferred to Subsequent Phase	The Transmission Service Provider that maintains CBM shall make available its current CBMID to the Transmission Operators, Transmission Service Providers, Reliability Coordinators, Transmission Planners, Resource Planners, and Planning Coordinators that are within or adjacent to the Transmission Service Provider's area, and to the Load Serving Entities and Balancing Authorities within the Transmission Service Provider's area, and notify those entities of any changes to the CBMID prior to the effective date of the change.
MOD-004-1	R3.	Deferred to Subsequent Phase	Each Load-Serving Entity determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by:

Standard Version	Requirement Name	Status	Requirement Text
MOD-004-1	R3.1.	Deferred to Subsequent Phase	Using one or more of the following to determine the GCIR: Loss of Load Expectation (LOLE) studies; Loss of Load Probability (LOLP) studies; Deterministic risk-analysis studies; Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R3.2.	Deferred to Subsequent Phase	Identifying expected import path(s) or source region(s).
MOD-004-1	R4.	Deferred to Subsequent Phase	Each Resource Planner determining the need for Transmission capacity to be set aside as CBM for imports into a Balancing Authority Area shall determine that need by:
MOD-004-1	R4.1.	Deferred to Subsequent Phase	Using one or more of the following to determine the GCIR: Loss of Load Expectation (LOLE) studies; Loss of Load Probability (LOLP) studies; Deterministic risk-analysis studies; Reserve margin or resource adequacy requirements established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R4.2.	Deferred to Subsequent Phase	Identifying expected import path(s) or source region(s).
MOD-004-1	R5.	Deferred to Subsequent Phase	At least every 13 months, the Transmission Service Provider that maintains CBM shall establish a CBM value for each ATC Path or Flowgate to be used for ATC or Available Flowgate Capability (AFC) calculations during the 13 full calendar months (months 2-14) following the current month (the month in which the Transmission Service Provider is establishing the CBM values). This value shall:
MOD-004-1	R5.1.	Deferred to Subsequent Phase	Reflect consideration of each of the following if available: Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Service Provider's area; Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Service Provider’s area; Any reserve margin or resource adequacy requirements for loads within the Transmission Service Provider’s area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R5.2.	Deferred to Subsequent Phase	Be allocated as follows: For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners; For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Service Provider

Standard Version	Requirement Name	Status	Requirement Text
MOD-004-1	R6.	Deferred to Subsequent Phase	At least every 13 months, the Transmission Planner shall establish a CBM value for each ATC Path or Flowgate to be used in planning during each of the full calendar years two through ten following the current year (the year in which the Transmission Planner is establishing the CBM values). This value shall:
MOD-004-1	R6.1.	Deferred to Subsequent Phase	Reflect consideration of each of the following if available: Any studies (as described in R3.1) performed by Load-Serving Entities for loads within the Transmission Planner's area; Any studies (as described in R4.1) performed by Resource Planners for loads within the Transmission Planner's area; Any reserve margin or resource adequacy requirements for loads within the Transmission Planner's area established by other entities, such as municipalities, state commissions, regional transmission organizations, independent system operators, Regional Reliability Organizations, or regional entities
MOD-004-1	R6.2.	Deferred to Subsequent Phase	Be allocated as follows: For ATC Paths, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners; For Flowgates, based on the expected import paths or source regions provided by Load-Serving Entities or Resource Planners and the distribution factors associated with those paths or regions, as determined by the Transmission Planner.
MOD-004-1	R7.	Deferred to Subsequent Phase	Less than 31 calendar days after the establishment of CBM, the Transmission Service Provider that maintains CBM shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the Transmission Service Provider's system of the amount of CBM set aside.
MOD-004-1	R8.	Deferred to Subsequent Phase	Less than 31 calendar days after the establishment of CBM, the Transmission Planner shall notify all the Load-Serving Entities and Resource Planners that determined they had a need for CBM on the system being planned by the Transmission Planner of the amount of CBM set aside.
MOD-004-1	R9.	Deferred to Subsequent Phase	The Transmission Service Provider that maintains CBM and the Transmission Planner shall each provide (subject to confidentiality and security requirements) copies of the applicable supporting data, including any models, used for determining CBM or allocating CBM over each ATC Path or Flowgate to the following:
MOD-004-1	R10.	Deferred to Subsequent Phase	The Load-Serving Entity or Balancing Authority shall request to import energy over firm Transfer Capability set aside as CBM only when experiencing a declared NERC Energy Emergency Alert (EEA) 2 or higher.
MOD-004-1	R11.	Deferred to Subsequent Phase	When reviewing an Arranged Interchange using CBM, all Balancing Authorities and Transmission Service Providers shall waive, within the bounds of reliable operation, any Real-time timing and ramping requirements.

Standard Version	Requirement Name	Status	Requirement Text
MOD-004-1	R12.	Deferred to Subsequent Phase	The Transmission Service Provider that maintains CBM shall approve, within the bounds of reliable operation, any Arranged Interchange using CBM that is submitted by an “energy deficient entity” under an EEA 2 if:
MOD-004-1	R12.1.	Deferred to Subsequent Phase	The CBM is available
MOD-004-1	R12.2.	Deferred to Subsequent Phase	The EEA 2 is declared within the Balancing Authority Area of the “energy deficient entity,” and
MOD-004-1	R12.3.	Deferred to Subsequent Phase	The Load of the “energy deficient entity” is located within the Transmission Service Provider’s area.
MOD-004-1	R9.1.	Deferred to Subsequent Phase	Each of its associated Transmission Operators within 30 calendar days of their making a request for the data.
MOD-004-1	R9.2.	Deferred to Subsequent Phase	To any Transmission Service Provider, Reliability Coordinator, Transmission Planner, Resource Planner, or Planning Coordinator within 30 calendar days of their making a request for the data.
NUC-001-2	R9.1.	Kept in Final SAR for Retirement	Administrative elements:
NUC-001-2	R9.1.1.	Kept in Final SAR for Retirement	Definitions of key terms used in the agreement.
NUC-001-2	R9.1.2.	Kept in Final SAR for Retirement	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.
NUC-001-2	R9.1.3.	Kept in Final SAR for Retirement	A requirement to review the agreement(s) at least every three years.
NUC-001-2	R9.1.4.	Kept in Final SAR for Retirement	A dispute resolution mechanism.
PRC-008-0	R1.	Kept in Final SAR for Information Only	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.
PRC-008-0	R2.	Kept in Final SAR for Information Only	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).
PRC-009-0	R1.	Kept in Final SAR for Information Only	The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization’s UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:

Standard Version	Requirement Name	Status	Requirement Text
PRC-009-0	R1.1.	Kept in Final SAR for Information Only	A description of the event including initiating conditions.
PRC-009-0	R1.2.	Kept in Final SAR for Information Only	A review of the UFLS set points and tripping times.
PRC-009-0	R1.3.	Kept in Final SAR for Information Only	A simulation of the event.
PRC-009-0	R1.4.	Kept in Final SAR for Information Only	A summary of the findings.
PRC-009-0	R2.	Kept in Final SAR for Information Only	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.
PRC-010-0	R2.	Kept in Final SAR for Retirement	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).
PRC-022-1	R2.	Kept in Final SAR for Retirement	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.
TOP-001-1a	R3.	Kept in Final SAR for Information Only	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.
TOP-005-2a	R1.	Kept in Final SAR for Information Only	As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for “Electric System Reliability Data.”

Standard Version	Requirement Name	Status	Requirement Text
VAR-001-2	R5.	Added to Final SAR for Retirement	Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.
VAR-002-WECC-1	R2.	Deferred to Subsequent Phase	Generator Operators and Transmission Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.10.
VAR-501-WECC-1	R2.	Deferred to Subsequent Phase	Generator Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.12.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2013-02 Retirement of Reliability Standard Requirements

Unofficial Comment Form for Paragraph 81 (P81) Project —Retirement of Reliability Standard Requirements

This form is provided in a Word format for the development of your internal drafts only.

Please use the electronic comment form located at the link below to submit official comments on the P81 Project. Comments must be submitted by **December 10, 2012.** If you have questions, please contact Kristin Iwanechko at Kristin.Iwanechko@nerc.net or by telephone at 404-446-9736.

http://www.nerc.com/filez/standards/Project2013-02_Paragraph_81.html

Background Information:
On September 30, 2011, the North American Electric Reliability Corporation (NERC) filed a petition with the Federal Energy Regulatory Commission (FERC) requesting approval of its proposal to make informational filings in a "Find, Fix, Track and Report" (FFT) spreadsheet of lesser-risk, remediated possible violations of Reliability Standards. On March 15, 2012, the FERC issued an order conditionally accepting NERC's FFT proposal. In paragraph 81 (P81) of that order, the FERC stated:

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently. *North American Electric Reliability Corporation,* 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, a draft Standards Authorization Request (SAR) was drafted to set forth criteria and a process to identify Reliability Standard requirements that either: (a) provide little protection to the Bulk Electric System; (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file the identified Reliability Standard requirements with FERC to have them removed from the FERC-approved list of Reliability Standards.

Standards Process Input Group (SPIG)

In addition to addressing P81, the draft SAR was drafted consistent with what the SPIG developed as Recommendation No. 4, as set forth in *NERC's Recommendations to Improve The Standards Development Process* on page *12* (April 2012), which states:

> Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

Collaborative Process

The draft SAR and a suggested list of Reliability Standard requirements embedded in the SAR for consideration in the Initial Phase was the product of collaborative discussions among the following entities and their members: Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group. The draft SAR was posted for comment, which were due September 4, 2012. The P81 Standards Drafting Team reviewed the comments and finalized the SAR and the proposed list of Reliability Standard requirements for retirement.

Proposed List

A list of Reliability Standard requirements proposed for retirement is posted along with a technical white paper that sets forth the technical justifications for each requirement. To obtain input on the list of Reliability Standard requirements proposed for retirement and the technical white paper, each are posted for a 45-day comment period. Accordingly, it is requested that you submit your comments by **December 10, 2012** via the electronic comment form.

Questions

1. **If retired, do any Reliability Standard requirements proposed for retirement create a gap in reliability?**

   If yes, please explain in the comment area.

   ☐ Yes

   ☐ No

   Comments:

2. **Do you have any comments on the technical white paper?**

   ☐ Yes

   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-02 Paragraph 81

Initial Ballot now open through 8 p.m. Monday, December 10, 2012

Now Available

An initial ballot for the 22 standards with 38 requirements being proposed for retirement in this project is open through **8 p.m. Eastern on Monday, December 10, 2012**.

The following documents are posted on the project page for review and balloting:

- **Redline of Standards with Proposed Retirements** – A PDF document containing a redline of each of the affected standards, indicating the requirements and associated elements proposed to be retired with a "(Retired)" and with the version number remaining the same. When these Requirements are retired, the version numbers of the standards will NOT be incremented. After evaluating the options and consulting with the Standards Committee and Standards Committee Process Subcommittee, the P81 drafting team determined that this was the most practical approach. Incrementing the version numbers of each standard is impractical because, in some cases, a subsequent version has already been developed. In addition, incrementing the version would require renumbering Requirements where a retired Requirement created a gap in numbering, and this creates an undesirable administrative burden for entities using certain systems to manage their compliance programs.
- **Implementation Plan** – The implementation plan for retiring the Phase I requirements.

Instructions

Members of the ballot pool associated with this project may log in and submit their vote for, by clicking here.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the list of requirements being proposed for retirement. If the comments do not show the need for significant revisions, the standards with requirements being proposed for retirement will proceed to a recirculation ballot.

Background

On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated the following in P81:

> "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES," are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.

The draft SAR, which included criteria for retiring or modifying requirements, defined phases for the project, and a suggested list of requirements put together by NERC, the regions, and the trades and their member companies for consideration in Phase I, was posted for an informal comment period. In September, the P81 SDT met to respond to the comments received and finalize the SAR. The revisions resulted in a list of 38 requirements in 22 Reliability Standard versions being proposed for retirement and an additional 13 requirements included for informational purposes only. The P81 SDT also developed a Technical White Paper which includes the justification for retiring the proposed requirements.

To sign up for the plus list for this project to follow along with meetings and work products, please email Kristin Iwanechko.

Standards Development Process

The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson,

Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-02 Paragraph 81

Formal Comment Period Now Open: October 25 – December 10, 2012
Ballot Pool Forming Now: October 25 – November 23, 2012

Upcoming
Initial Ballot: November 30 – December 10, 2012

Now Available

The Paragraph 81 (P81) standard drafting team (SDT) has posted a single PDF containing redlined versions of 27 standards showing 38 requirements proposed to be retired, and an implementation plan for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Monday, December 10, 2012. A ballot pool is being formed and the ballot pool window is open through 8 a.m. Eastern on **Friday, November 23, 2012** (*please note that ballot pools close at 8 a.m. Eastern and mark your calendar accordingly*).

The following documents are posted on the project page for review and balloting:

- **Redline of Standards with Proposed Retirements** – A PDF document containing a redline of each of the affected standards, indicating the requirements and associated elements proposed to be retired with a "(Retired)" and with the version number remaining the same. When these Requirements are retired, the version numbers of the standards will NOT be incremented. After evaluating the options and consulting with the Standards Committee and Standards Committee Process Subcommittee, the P81 drafting team determined that this was the most practical approach. Incrementing the version numbers of each standard is impractical because, in some cases, a subsequent version has already been developed. In addition, incrementing the version would require renumbering Requirements where a retired Requirement created a gap in numbering, and this creates an undesirable administrative burden for entities using certain systems to manage their compliance programs.
- **Implementation Plan** – The implementation plan for retiring the Phase I requirements.

The following documents are posted on the project page as Supporting Materials to assist stakeholders in their review:

- **Final SAR (clean and redline)** – The final SAR incorporates revisions to the draft SAR by the P81 SDT in response to comments received from the industry.
- **Technical White Paper** – The technical white paper includes the technical justification developed by the P81 SDT to support the retirement of the proposed requirements in Phase I.

- **Redline of VSL Matrix** – This identifies the VSLs (and parts of VSLs) that will be retired when the requirements in Phase I are retired. The matrix may be useful in providing a complete view of the VSLs and parts of VSLs that will be retired when a particular Requirement is retired, since some of the early standards have not had the FERC-approved VSLs incorporated in the standard.
- **Spreadsheet with Proposed Retirements** – This spreadsheet includes a list of the requirements proposed in the draft SAR and their status in the final SAR (kept in final SAR for retirement, kept in final SAR for information only, deferred to subsequent phase). Additionally, the spreadsheet includes requirements that were added to the Phase I list as a result of industry comments on the draft SAR, which are identified as 'added to final SAR for retirement.'
- **Unofficial Comment Form (Word)** – A Word version of the comment form for the development of internal draft responses only (the final must be submitted electronically).

Instructions for Joining Ballot Pool(s)

Registered Ballot Body members must join the ballot pool to be eligible to vote in balloting of the requirements being proposed for retirement. A single ballot pool is being formed, and all of the standards with Requirements being proposed for retirement will be balloted as a group. Registered Ballot Body members may join the ballot pool at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using the "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list server.) The ballot pool list server for this ballot pool is: bp-2013-02_P81_in@nerc.com.

The ballot pool is open **through 8 a.m. Eastern on Friday, November 23, 2012.**

Instructions for Commenting

A formal comment period is open through 8 p.m. Eastern on **Monday, December 10, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

A single ballot for all of the standards with Requirements being proposed for retirements will be conducted Friday, November 30, 2012 through 8 p.m. Monday December 10, 2012.

Background

On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated the following in P81:

> "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES," are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.

The draft SAR, which included criteria for retiring or modifying requirements, defined phases for the project, and a suggested list of requirements put together by NERC, the regions, and the trades and their member companies for consideration in Phase I, was posted for an informal comment period. In September, the P81 SDT met to respond to the comments received and finalize the SAR. The revisions resulted in a list of 38 requirements in 23 Reliability Standard versions being proposed for retirement and an additional 13 requirements included for informational purposes only. The P81 SDT also developed a Technical White Paper which includes the justification for retiring the proposed requirements.

To sign up for the plus list for this project to follow along with meetings and work products, please email Kristin Iwanechko.

Standards Development Process

The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-02 Paragraph 81

Initial Ballot Results

Now Available

An initial ballot for the 22 standards with 38 requirements being proposed for retirement in this project concluded at **8 p.m. Eastern on Monday, December 10, 2012**.

Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results.

Approval
Quorum: 75.77% Approval: 96.45%

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the list of requirements being proposed for retirement. If the comments do not show the need for significant revisions, the standards with requirements being proposed for retirement will proceed to a recirculation ballot.

Background

On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated the following in P81:

> "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability

> Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES," are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.

The draft SAR, which included criteria for retiring or modifying requirements, defined phases for the project, and a suggested list of requirements put together by NERC, the regions, and the trades and their member companies for consideration in Phase I, was posted for an informal comment period. In September, the P81 SDT met to respond to the comments received and finalize the SAR. The revisions resulted in a list of 38 requirements in 22 Reliability Standard versions being proposed for retirement and an additional 13 requirements included for informational purposes only. The P81 SDT also developed a Technical White Paper which includes the justification for retiring the proposed requirements.

To sign up for the plus list for this project to follow along with meetings and work products, please email Kristin Iwanechko.

Standards Development Process

The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results

Ballot Name:	Project 2013-02 Paragraph 81 Initial Ballot October 2012_in
Ballot Period:	11/30/2012 - 12/10/2012
Ballot Type:	Initial
Total # Votes:	319
Total Ballot Pool:	421
Quorum:	**75.77 % The Quorum has been reached**
Weighted Segment Vote:	96.45 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	112	1	83	0.976	2	0.024	2	25
2 - Segment 2.	10	0.8	7	0.7	1	0.1	1	1
3 - Segment 3.	98	1	69	0.986	1	0.014	3	25
4 - Segment 4.	37	1	21	1	0	0	2	14
5 - Segment 5.	94	1	70	0.986	1	0.014	0	23
6 - Segment 6.	51	1	43	1	0	0	0	8
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	9	0.7	7	0.7	0	0	0	2
9 - Segment 9.	3	0.1	1	0.1	0	0	0	2
10 - Segment 10.	7	0.5	4	0.4	1	0.1	0	2
Totals	**421**	**7.1**	**305**	**6.848**	**6**	**0.252**	**8**	**102**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1		Vijay Sankar		
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston		
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		
1	Colorado Springs Utilities	Paul Morland		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer	Affirmative	
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Long Island Power Authority	Robert Ganley		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees		
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	National Rural Electric Cooperative Association	Paul McCurley	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	

1	Omaha Public Power District	Doug Peterchuck		
1	Oncor Electric Delivery	Jen Fiegel		
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County, Washington	Rod Noteboom		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik		
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Steven Norris		
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Robert Lafferty		
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Buckeye Power, Inc.	Patrick O'Loughlin	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Hudson Gas & Electric Corp.	Thomas C Duffy	Negative	

3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Homestead	Orestes J Garcia		
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City of Ukiah	Colin Murphey	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan		
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	Richard Blumenstock	Abstain	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr		
3	East Kentucky Power Coop.	Patrick Woods	Affirmative	
3	Entergy	Joel T Plessinger		
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Danny Lindsey	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed		
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage		
3	Municipal Electric Authority of Georgia	Steven M. Jackson		
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Gary Clear		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	

3	Puget Sound Energy, Inc.	Erin Apperson		
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott		
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alabama Municipal Electric Authority	Raymond Phillips		
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Buckeye Power, Inc.	Manmohan K Sachdeva	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	
4	Consumers Energy	David Frank Ronk	Abstain	
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	LaGen	Richard Comeaux		
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Turlock Irrigation District	Steven C Hill		
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Corp	George Tatar	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		

5	Bridgeport Energy	Cleyton Tewksbury		
5	Buckeye Power, Inc.	Paul M Jackson	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Grand Island	Jeff Mead	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative	
5	Colorado Springs Utilities	Jennifer Eckels		
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl		
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	East Kentucky Power Coop.	Stephen Ricker	Affirmative	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer		
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Essential Power, LLC	Patrick Brown	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	ExxonMobil Research and Engineering	Martin Kaufman	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard		
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego		
5	MidAmerican Energy Co.	Neil D Hammer	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Laurel Heacock		
5	Oklahoma Gas and Electric Co.	Kim Morphis	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	Colin Anderson	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	PacifiCorp	Bonnie Marino-Blair	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Affirmative	

5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Affirmative	
5	Southern California Edison Company	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer		
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn		
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	Modesto Irrigation District	James McFall		
6	Muscatine Power & Water	John Stolley	Affirmative	
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried		
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Kelly Cumiskey	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Ty Bettis	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	

6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
9	New York State Department of Public Service	Thomas G. Dvorsky		
10	Midwest Reliability Organization	William S Smith		
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	

Individual or group. (32 Responses)
Name (19 Responses)
Organization (19 Responses)
Group Name (13 Responses)
Lead Contact (13 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (1 Responses)
Comments (32 Responses)
Question 1 (30 Responses)
Question 1 Comments (31 Responses)
Question 2 (31 Responses)
Question 2 Comments (31 Responses)

Group
Arizona Public Service Company
Jana Van Ness, Director of Regulatory Compliance
No
No
Individual
Thomas C. Duffy
Central Hudson Gas & Electric Corporation
No
Yes
CHG&E believes the reason for retiring CIP-003-3,-4 R3 and its sub-requirements is fallacious. The reason provided in the technical white paper is essentially: " First, and most importantly, that requirement has never been available for use to exempt an entity form compliance with any requirement of any NERC reliability standard. It only applies to exceptions to internal corporate policy, and only in cases where the policy exceeds a NERC standard requirement, or addresses an issue that is not covered in a NERC reliability standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of 8 characters in length, and be changed every 30 days, this provision could be used for internal governance purposes to lessen the corporate requirement, back to the password requirements in CIP-007 R5.3, or in conjunction with a TFE to something else. The removal of this requirement has no effect on the TFE process, or compliance with any other NERC reliability standard requirement." CHG&E wishes to highlight the fact that NERC has no jurisdiction to impose or grant exceptions to internal corporate policies. Therefore, this requirement (and its sub – requirements) can only have been crafted to address exceptions to the NERC CIP requirements. Throughout this standard, the NERC requirements for a 'cyber security policy' are delineated. This requirement specifically addresses exceptions to the 'cyber security policy'. As written, this requirement can only be interpreted to mean that an exception to the NERC CIP required 'cyber security policy' is acceptable if properly documented and approved by the CIP Senior Manager. Central Hudson Gas & Electric Corporation strongly disagrees with the inclusion of CIP-003-3, -4 Requirements R3, R3.1, R3.2, R3.3 as candidates for retirement. The reasons stated in the SAR in favor of inclusion are that these requirements are administrative in nature and are purely examples of a documentation process. Further it is stated in the SAR that they, "…. have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements." This last statement is precisely the reason why the aforementioned requirements were included in the standard. These requirements allow Registered Entities to, on rare occasions, take an exception to one or several of the CIP requirements (for a

limited period of time) if they (1) have valid cause (major emergency, Force Majeure, etc.), (2) document the occurrence and (3) are reviewed and approved by the CIP Senior Manager. This process supports the Registered Entity's compliance effort and acknowledges the need for special protocols to address emergency circumstances. Without such a process, the only recourse for the Registered Entity is to self-report a violation which is not within their control. In other words, retirement of these requirements would force the Registered Entity to be in full compliance with ALL CIP Standards ALL the time regardless of circumstance. The concept of realistic expectations was undoubtedly the reason these requirements were crafted and included in the standard. Further, with regard to the Registered Entity's decision to claim an exception, a system of checks and balances already exists. At the time of a compliance audit of the standard's requirements, the Regional Entity reviews and makes a determination as to whether the actions taken by the Registered Entity were warranted. Further, the fact that this requirement is included in the FFT process is of little consolation since any exception would still constitute a violation of the NERC Standard on the part of the Registered Entity and would carry with that violation the associated stakeholder liability.
Individual
David Ramkalawan
Ontario Power Generation
No
The technical white paper has provided reasonable and well thought-out justifications for the retirement proposal to those reliability standard requirements.
No
Individual
John Bee
Exelon
Exelon agrees with EEIs position and comments submitted related to this project.
Yes
Exelon believes that if a company takes an exception it should be documented and proposes the following revision to R3: R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented. R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
No
Group
Northeast Power Coordinating Council
Guy Zito
No
No
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
Please note: CIP-001-2a EA4 should be retired at the same time as CIP-001-2a R4 for the same reasons. We agree with the SDT regarding requirements applicable to the GO/GOP.
Yes

Please note: CIP-001-2a EA4 should be retired at the same time as CIP-001-2a R4 for the same reasons. We agree with the SDT regarding requirements applicable to the GO/GOP.
Group
Imperial Irrigation District (IID)
Jesus Sammy Alcaraz
No
No
Individual
Andrew Z. Pusztai
American Transmission Company
No
No
Group
Duke Energy
Greg Rowland
No
Yes
While we agree with retiring all of the Reliability Standard requirements proposed for retirement, we believe the P81 Project Technical White Paper should be more forceful in justifying retirement of the CIP requirements. Specifically, the "not an important part of a scheme of CIP Requirements" phrase is often used in Criteria C sections discussing VFR and AML issues. It would seem that FERC may have difficulty giving this phrase credibility since (i) the industry previously had balloted to approve such requirements, (ii) NERC BOT approved such requirements, and (iii) FERC approved such requirements. All of these approvals seem to indicate that all such entities previously believed that the requirements were important to the CIP scheme. Instead, we suggest that this phrase be replaced in each instance with phrases like the following: "As explained above and since the inception of this requirement, this requirement has not been shown to constitute a [key][integral] part of a scheme of CIP requirements."
Individual
Nazra Gladu
Manitoba Hydro
No
Standard revision numbers and Requirement sequence changes should be made at a later date, as future revisions are required to each Standard that contains any retired Requirements. This will relieve the undesirable administrative burden, while reflecting accurate revision numbers and Requirement sequences, as changes are required to the Standards.
Yes
CIP-003-3,-4 R1.2: Technical Justification (page 19): CIP personnel should act based on their cyber security policy; a policy which must address the CIP-002 through CIP-009 standards as required by CIP-003 R1.1. As a result, the specific training processes and procedures will reflect the cyber security policy. We suggest "they will act via their specific training, processes and procedures which reflect the overarching cyber security policy." CIP-007-3, -4 R7.3: (1) Technical Justification (page 32): For

added clarity, we suggest the wording "… small number of Reliability Standard requirements explicitly mandating ….". (2) Data and information collection for ERO compliance monitoring purposes is certainly within the context of the Reliability Standards. For added clarity, we suggest the wording "... for ERO compliance monitoring purposes without specific data collection language in the Reliability Standards." (3) It is unclear who "the entities" are. Should this state "Responsible Entities"? (4) For additional clarity, we suggest the wording "... the Reliability Standards are arguably more difficult to understand ...".
Individual
David Jendras
Ameren
No
No
Individual
Patrick Brown
Essential Power, LLC
No
No
Individual
David Thorne
Pepco Holdings Inc.
No
Yes
As part of this effort, a new revision number for any standard that is changed should be used. Also any measurements or registered entities (e.g. RRO) that would no longer apply should be deleted.
Group
Bonneville Power Administration
Jamison Dye
No
Yes
BPA appreciates the drafting team's decision to include TOP-001-1 R3 in the technical white paper for informational purposes rather than proposing to retire it.
Group
Dominion Resource Services
Randall Heise
No
No
Individual

Thad Ness
American Electric Power
No
AEP is not aware of any reliability gaps that would occur as a result of retiring the proposed Reliability Standards requirements.
No
Individual
Michelle D'Antuono
Occidental Energy Ventures Corp.
No
Occidental Energy Ventures Corp ("OEVC"). believes that the retirement of the Phase I requirements will pose little, if any, risk to the BES. However, in our view, this is a good start to a much more extensive restructuring of the regulatory model. Of course, the industry will need to gauge FERC's response to the initial grouping of requirements, but we should be prepared to aggressively push down this path.
Yes
OEVC believes the drafting team did an excellent job researching and defending each proposed retirement. In our view, this is a fundamental necessity as we must assume that FERC will closely scrutinize each one. However, we anticipate that some form of cost/benefit analysis will be requested in each case – particularly since the entire impetus behind the Paragraph 81 project is the shortage of compliance resources. It may be a worthwhile exercise to develop a cost model that accounts for industry and CEA resources accurately and effectively. The results must be weighed against the expected benefit of any requirement – as the industry and regulatory bodies clearly have some important trade-offs to consider. In particular, with FERC's recent emphasis on cyber security, cold weather preparation, and geomagnetic protection, some of the less effective requirements need to be removed. OEVC believes that the Commission will be reluctant to proceed in this manner without data that demonstrates the comparative benefit of each requirement.
Individual
Patricia Metro
National Rural Electric Cooperative Association (NRECA)
No
Yes
NRECA is very supportive of the recent ERO, Regional Entities and industry stakeholder efforts in response to the opportunity provided by FERC in P81 of the Find, Fix, Track and Report Order to review and eliminate standard requirements that provide no or minimal reliability benefits. NRECA is disappointed with the small number of requirements that are proposed for retirement in this initial phase of work, but will support this effort as it moves through the NERC standards development process and will continue participating in future phases of work related to the P81 project. It is our goal to ensure future phases of this effort lead to retirement of a much greater number of requirements that are not necessary for the reliability of the Bulk Electric System. NRECA has reviewed the P81 Technical White Paper. It appears that there are many more requirements, in addition to the 38 identified, that meet the criteria for deletion most of which were included in the SAR for this project. Although the phase approach to this project was explained and many of the requirements included in the SAR will be addressed in a subsequent phases of the project, there is a concern that the future phases of the project will not be completed in a timely manner since there is no timeline provided for the future phases in the Implementation Plan for this project. Having such a time-line will demonstrate to the FERC that the industry and the ERO are dedicated to eliminating standard requirements that provide no or minimal reliability benefits. NRECA is concerned that drafting teams are drafting requirements that would meet the criteria for deletion stated in this

Technical White Paper. There must be a mechanism in place to ensure "P81-qualified" requirements are not included in standards that are under development or in standards that are provided to the NERC BOT for approval. In addition, if requirements are retired that include an entity that is only required to comply with the standard because of the specific requirement that is to be retired said entity should be removed from the applicability of the standard. An example of such is VAR-01, R5 where this requirement is the only requirement applicable to a PSE, but the PSE has not been removed from the Applicability of the standard in the red-line version posted for comment.
Group
Hydro One Networks Inc.
Sasa Maljukan
No
Yes
Hydro One very much appreciates the efforts of the SDT in trying to streamline and focus current standards to focus on requirement that impact to reliability. In addition to this, we hope that: - Phase II of this project will continue along the same path and advance the approach to other approved standards, and - Work on new and reviewed standards will include the criteria developed in this project (i.e. SDTs are fully directed to use Paragraph 81 criteria while developing new and reviewing existing standards).
Group
SERC EC Planning Standards Subcommittee
Jim Kelley
No
The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers"
No
The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers"
Individual
Kathleen Goodman
ISO New England Inc.
Agree
ISO RTO Council Standards Review Committee (SRC)
Group
SPP Standards Review Group
Robert Rhodes
No
Yes
Page 17 – The 6th through 12th lines are a stretch and do not add anything to the argument for retiring Requirement 3 of CIP-001-2a. It is conjecture on the part of the drafting team and should be removed from the paper. If the drafting team doesn't agree and keeps this portion, please insert the word 'require' between 'some' and 'corporate' in the 8th line. Also, delete 'to generic' in the 11th line. Page 26 – In the 10th line of the Technical Justification paragraph, insert 'task' between 'administrative' and 'that'. Page 29 – At the beginning of the 6th line of the Technical Justification paragraph, delete the 'is'. Page 32 – In the first line of the Criterion A paragraph, insert a 'not' between 'does' and 'promote'. Page 59 – In the 8th line of the 2nd paragraph, the sentence 'Thus,

IRO-016-1 R1 does not support reliability.' doesn't seem right. Shouldn't this be; it does support reliability? Or perhaps you meant to say that R2 does not support reliability. Also, in the next sentence, delete the second 'that'. Page 61 – In the 15th line of the Technical Justification paragraph, delete the 'an' in front of unnecessarily.

Individual

Michael Falvo

Independent Electricity System Operator

Yes

1. BAL-005-0.2b, R2 – agree 2. CIP-001-2a, R4 – we do not agree this is administrative in nature. Preparedness is an essential element in having the capability to readily respond to pressing reliability issues. Establishing contact with the enforcement authorities is a necessary component in preparing for reporting suspect or detected sabotage. Such reporting can help protect or minimize damages to BES facilities and/or Adverse Reliability Impact due to malicious acts. R1 to R3 do not have such a requirement to report sabotage events to the law enforcement authorities. If these authorities are included in Requirement R3, then the gap may be considered filled and R4 can be retired. However, this is not yet the case. We therefore suggest that R4 not be retired at this time. 3. CIP-003-3, -4 R1.2 – agree 4. CIP-003-3, -4 R3, R3.1, R3.2, R3.3 – while we agree that having the exception documented and approved by Senior Manager adds little to reliability, we do not agree that the entire requirement should be removed since this requirement is intended for implementing control of an entity's adherence to its Cyber Security policy, or document exceptions otherwise. Further, we do not concur with the SDT's view that over time, responsible entities may believe they can exempt themselves from compliance with the CIP requirements. Entities may exempt themselves from having some of their processes/procedures for cyber security not implemented, but their adherence to the policy and documenting exceptions are to be assessed during audit, which is not determined by the entities themselves. Any deviation from the requirement (the proposed "making exemption from compliance with the CIP requirement") will be identified and the entities will be found non-compliant. 5. CIP-003-3, -4 R4.2 – we agree that the action to classify the CCA information is redundant, but we do not think R4.2 can be removed entirely since the element "based on the sensitivity of the Critical Cyber Asset information" needs to be retained. Suggest to revise R4 to capture this element, or, at a minimum, consult the CIP SDT on the merit of retaining this element in R4. 6. CIP-005-3a, -4a R2.6 – agree. 7. CIP-007-3, -4 R7.3 – agree. 8. COM 001-1.1 R6 - agree. 9. EOP-004-1 R1 – we do not agree with retiring this requirement. The RRO should have a formal reporting procedure in place to ensure adequate and detailed reporting is provided on system disturbances or any unusual event. This procedure is necessary for entities to meet the goals of further requirements in this standard that pertain to preliminary and final disturbance reporting . 10. EOP-005-2 R3.1 – agree. 11. EOP-009-0 R2 – agree. 12. FAC-002-1 R2 – we do not agree that the requirement is burdensome. The requirement seems to meet the overarching criterion A from the White Paper (it requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES), however, at a careful reading, the requirement seems to fail meeting at least one of the Criteria B: B1 (it is administrative, but not burdensome), B2 (it is data collection/retention, but we are not sure if NERC collects this data by any other method), B3 to B6 (it does not seem to fit any of these criteria). 13. FAC-008-1 R1.3.5 – agree. 14. FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5 – agree. 15. FAC-010-2.1 R5; FAC-011-2 R5 – agree. 16. FAC-013-2 R3 – agree. 17. INT-007-1 R1.2 – agree, but there needs to be a requirement somewhere to stipulate that all entities involved in the Arranged Interchange must register with NERC such that transactions' participants can be contacted for confirmation of transactions being approved or to make changes when transactions are curtailed. Until such time that this requirement is developed elsewhere, INT-007-1 R1.2 should remain in effect. 18. IRO-016-1 R2 – It does not make sense to retire this requirement, but still keep M1 – the measure associated with requirement R1 - in the standard. M1 states that each RC must have evidence, such as operator log or another data source, of actions taken for the event or disagreement or both. However, R2 is the requirement which states the RC shall document the actions taken via operator log or another data source. Therefore, removing R2 would create inconsistency in the standard. 19. NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4 we agree with retiring all of the 9.1, except R9.1.2: The agreement should contain the names of the applicable entities and the responsibilities assigned to each one in relation to the NPIR. 20. PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1;

PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 – agree. 21. TOP-001-1a R3 – agree. 22. TOP-005-2a R1 – agree. 23. VAR-001-2 R5 – agree.
No
Individual
Orlando Ciniglio
Idaho Power Company
No
No
Group
ACES Standards Collaborators
Jason Marshall
No
(1) We do not see any reliability gaps created by the proposed retirements. Many of the requirements that have been moved to the second phase of the project could actually be retired in this phase without creating reliability gaps. We believe the approach to move several requirements to the second phase is overly conservative. However, we understand that drafting team must balance the retirement of requirements in this phase with satisfying concerns of stakeholders that no reliability gaps are created. (2) We are not opposed to the plan to review the linkages between BAL and INT standards in the next phase. However, we continue to believe that reloading of curtailed transactions is a commercial issue not a reliability issue. Thus, INT-004-2 easily meets criteria A and B and should be retired in phase one.
Yes
(1) On page 5, several requirements are marked with two asterisks but there is no footnote or additional information. Please indicate the purpose of the asterisks or remove them. (2) The supporting statement in the technical whitepaper and SAR that Criteria C is needed to make an informed decision "in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B" is inconsistent with the actual Criteria. Criterion C2 questions if the requirement is being reviewed in an on-going standards development project. While this is certainly a relevant question and a valid reason to not include a requirement in the P81 project, the question simply provides no input on whether Criteria A and B are met. We suggest changing the supporting statement to be clearer that Criteria C in essence is more information to make an informed decision but may not necessarily have any indication on whether Criteria A and B are satisfied. (3) The supporting statement in the technical whitepaper and SAR that Criteria C provides "additional information to assist in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B" is inconsistent with the SAR. In the detailed description, the SAR states that the initial phase shall only identify requirements that satisfy both Criteria A and B. These are supposed to be the requirements that easily meet these two criteria sets. Thus, why is Criteria C evaluated in the whitepaper. If these criteria are easily met, Criteria C is not needed to assist in the determination and the associated information while interesting would appear to be superfluous.
Group
Southwest Power Pool Regional Entity
Emily Pennel
No
While CIP-007-3/4, Requirement R7.3 by itself has no immediate impact on the reliability of the Bulk Electric System, performance of R7.3 is required by the entity in order to be able to demonstrate compliance with CIP-007-3, Requirements R7.1 and R7.2 that, if not performed properly, could result in an impact to reliability. Elimination of this requirement could expose the registered entity to greater

risk of non-compliance with the remaining requirements as it no longer requires the entity to maintain appropriate and sufficient evidence of performance with the remaining requirements. For the reasons described, the SPP RE is opposed to retiring CIP-007-3/4, Requirement R7.3.
Yes
The white paper discussion for CIP-007-3/4, Requirement R7.3 proffers the idea that most data and information is collected for ERO compliance monitoring purposes outside of the context of Reliability Standards. While this might be the case of other standards, the SPP RE does not believe this is the case for the CIP-002 through CIP-009 Cyber Security standards, collectively referred to as the "CIP standards." The CIP standards require the entity to produce a document (e.g., policy, program, procedure, process, or list); to implement a documented program, process, or procedure; and/or to perform and document certain measurable procedural steps. In the absence of disposition records, which are specifically not required by CIP-007-3/4, Requirements R7.1 and R7.2, there will unlikely be any data or information outside of the context of the Reliability Standards demonstrating compliance with R7.1 and R7.2. The authors of the white paper appear to object to the maintenance of process documentation in this instance yet do not object to other requirements in the CIP standards that similarly call for the production and maintenance of documentation. The SPP RE is concerned that the authors of the white paper have chosen to focus on individual requirements in a stand-alone manner and have failed to understand the supportive interrelationships of the CIP standards and their requirements.
Group
Southern Company
Antonio Grayson
No
Yes
FAC-002-1 R2-The comments in the technical white paper concerning FAC-002-1 R2 are correct. Entities already have the obligation to provide the documentation of the evaluation of the reliability impact of new facilities upon request to demonstrate compliance to R1 and its sub-requirements, thus making R2 unnecessary. Furthermore, a requirement to retain documentation does not benefit or protect the reliable operation of the BES. VAR-001-2 R5: While Southern agrees that the elimination of VAR-001-2, R5 is appropriate, there is some concern that the justification that the TOP's adherence to R2 as a double check to ensure there are sufficient reactive power resources to protect the voltage levels under normal and Contingency conditions may be viewed by FERC as redirecting the burden from the PSEs and LSEs to the TOP. The LSE's (particularly) need to make their reactive resources available to the TOP in order for the TOP to acquire/use these reactive resources to protect voltage levels. Also, consider that not all entities necessarily take service under a transmission tariff, so references to other contractual mechanisms such as Interchange Agreements, etc. might be cited in the Technical White Paper for ensuring sufficient reactive resources are provided and made available by transmission customers.
Individual
Brett Holland
Kansas City Power & Light
No
No
Individual
Jason Snodgrass
Georgia Transmission Corporation
No

Yes
GTC is very supportive of the recent ERO, Regional Entity and industry stakeholder efforts in response to the opportunity provided by FERC in paragraph 81 of the Find, Fix, Track and Report Order to review and eliminate standards that provide no or minimal reliability benefits. However, we are disappointed with the small number of requirements that are proposed for retirement in this initial phase of work. GTC would like to note that because duplicative requirements for subsequent versions of Reliability Standards are never mandatory at the same time, the net impact of requirements being proposed for retirement identified in the "Redline of Standards with Proposed Retirements" for phase 1 is only 28 out of 1650 FERC approved requirements or 1.7%. This small percentage does not seem to reflect well on the view that NERC's FFT initiative is predicated on, of which FERC has extended an invitation to justify without imposing a deadline. From our review of the P81 Technical White Paper, it appears that there are many more requirements in addition to the 28 identified that meet the criteria for deletion. And while a phased approach has been recommended, the certainty associated with subsequent phases occurring in a timely manner is questionable and GTC recommends a big picture approach. We believe the small number of requirements identified in phase I would be more palatable if a big picture perspective was provided once submitting to FERC. For example, a breakdown similar to the one below would provide more confidence that future phases would occur and be successful: • At the end of the day, we believe we can eliminate approximately xx number or xx percentage of requirements • This will be completed in three phases • Phase one will include approximately xx requirements, posted to FERC in fourth quarter, 2012 • Phase two will include approximately xx requirements, posted to FERC in xx quarter, 2013 • Phase three posting will… Laying out the bigger picture keeps the momentum going and also let's FERC know that the first posting only begins to scratch the surface of the issue. Furthermore, we are aware of current standards drafting teams that are drafting requirements that would meet the criteria for deletion stated in this Technical White Paper. There is a pressing need to implement a mechanism to ensure "P81-qualified" requirements are not drafted going forward or eliminated prior to NERC BOT approval. GTC will continue to support this effort as it moves through the NERC standards development process and participate in future phases of work related to the P81 project. Our goal is to ensure future phases of this effort lead to retirement of a much greater number of requirements that are not necessary for the reliability of the BES.
Individual
Daniela Hammons
CenterPoint Energy
No
CenterPoint Energy believes that the Reliability Standard requirements proposed for retirement in the initial phase ("Phase 1") of NERC Project 2013-02 'Paragraph 81' would not create a gap in reliability if they were retired. An increase in efficiency of the ERO compliance program should result with the removal of these Phase 1 requirements and the removal of additional Reliability Standard requirements in subsequent phases of this project.
No
Individual
Oliver Burke
Entergy Services, Inc. (Transmission)
No
No
Group
ISO/RTO Standards Review Committee
Albert DiCaprio

The SRC has not identified any reliability gaps caused by the proposed actions, but the SRC believes that there is value in retaining some of the deleted requirements in some other form. Documentation is not an Operating or Assessment obligation but it is a unique topic Chain-of-command should be addressed as a Certification issue or as a Assumption / Definition Issue The following requirements while not appropriate as mandatory Reliability Standards should be retained in some category (highlighted text is a proposed category) BAL-005-0.2b R2 (Current Industry Operating Practice) CIP-003-3 R1.2 CIP-003-3 R3 CIP-003-3 R4.2 CIP-003-4 R3 CIP-003-4 R3.1 CIP-003-4 R3.2 CIP-003-4 R3.3 CIP-003-4 R4.2 CIP-005-3a R2.6 CIP-005-4a R2.6 CIP-007-3 R7.3 CIP-007-4 R7.3 EOP-004-1 R1 (Industry Reports) EOP-005-2 R3.1 (Annual check-up / inspection) FAC-002-1 R2 --- FAC-008-1 R2 (Chain-of-Command) FAC-008-1 R3 --- FAC-008-3 R4 (Chain-of-Command) FAC-008-3 R5 --- FAC-010-2.1 R5** (Current Industry Assessment Practice) FAC-011-2 R5** (Current Industry Assessment Practice) FAC-013-2 R3 (Business Practice – NAESB) IRO-016-1 R2 (Documentation) NUC-001-2 R9.1 (Current Industry Operating Practice) NUC-001-2 R9.1.1 (Annual check-up / inspection) NUC-001-2 R9.1.2 (Documentation) NUC-001-2 R9.1.3 (Documentation) NUC-001-2 R9.1.4 (Certification) PRC-010-0 R2 (Current Industry Assessment Practice) PRC-022-1 R2 (Documentation) Please note the IESO will submit its own comments regarding the following requirements: CIP-001-2a R4 CIP-003-3 R3.1 CIP-003-3 R3.2 CIP-003-3 R3.3 CIP-003-4 R14.2 INT-007-1 R1.2 (Certification) VAR-001-2 R5** (Business Practice – NAESB)
Yes
The SRC agrees with the removal of the identified requirements. The SRC recognizes that the scope of this SAR is to identify inappropriate requirements and not necessarily to suggest what to do with those identified requirements for removal. The SRC suggests that the Technical White Paper recognize that some of these removed requirements can and should be retained (just not retained as Reliability Standards). See response to Q1 for suggestions.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2013-02 Paragraph 81

The Paragraph 81 Drafting Team thanks all commenters who submitted comments on the redlined versions of 22 standards showing 38 requirements proposed to be retired. The standards were posted for a 45-day public comment period from October 25, 2012 through December 10, 2012. Stakeholders were asked to provide feedback on the standards through a special electronic comment form. There were 32 sets of comments, including comments from approximately 113 different people from approximately 64 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Ben Wu	Orange and Rockland Utilities, Inc.	NPCC	1
3.	Greg Campoli	New York Independent System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Donald Weaver	New Brunswick System Operator	NPCC	2
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Wayne Sipperly	New York Power Authority	NPCC	5
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Christina Koncz	PSEG Power LLC	NPCC	5
12.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5
15.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
16.	Robert Pellegrini	The United Illuminating Company	NPCC	1
17.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
18.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
19.	Brian Robinson	Utility Services	NPCC	8
20.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
21.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3

2.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jose Landeros	IID	WECC	1, 3, 4, 5, 6
2.	Al Juarez	IID	WECC	1, 3, 4, 5, 6
3.	Marcela Caballero	IID	WECC	1, 3, 4, 5, 6
4.	Cathy Bretz	IID	WECC	1, 3, 4, 5, 6

3.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Lee Schuster	Duke Energy	FRCC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

4.	Group	Jamison Dye	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bart McManus	Technical Operations	WECC	1
2.	Ayodele Idowu	Technical Operations	WECC	1
3.	Daniel Goodrich	Technical Operations	WECC	1
4.	Tim Loepker	Dispatch	WECC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

5.	Forrest Krigbaum	System Operations	WECC	1
6.	Huy Ngo	Design & Maint	WECC	1
7.	John Wylder	Stds Montr & Admin	WECC	1
8.	Thomas Gist	Stds Montr & Admin	WECC	1
9.	Jenny Wilson	Transmission Planning	WECC	1
10.	Larry Furumasu	Transmission Planning	WECC	1
11.	Kyle Kohne	Transmission Planning	WECC	1
12.	Richard Becker	Substation Engineering	WECC	1
13.	Kieran Connolly	Generation Scheduling	WECC	5
14.	Erika Doot	Generation Support	WECC	3, 5, 6
15.	Deanna Phillips	FERC Compliance	WECC	1, 3, 5, 6

5.	Group	Randall Heise	Dominion Resource Services	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michael	Garton	MRO	5, 6
2.	Connie	Lowe	RFC	6
3.	Louis	Slade	RFC	5
4.	Randall	Heise	NPCC	5, 6
5.	Michael	Crowley	SERC	5, 1, 3

6.	Group	Sasa Maljukan	Hydro One Networks Inc.	X									

	Additional Member	Additional Organization	Region	Segment Selection
1.	David kiguel	Hydro One Networks Inc.	NPCC	1

7.	Group	Jim Kelley	SERC EC Planning Standards Subcommittee	X				X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Sullivan	Ameren Services Company	SERC	1
2.	Charles Long	Entergy Services, Inc.	SERC	1
3.	Edin Habibovich	Entergy Services, Inc.	SERC	1
4.	James Manning	NC Electric Membership Cooperation	SERC	1
5.	Philip Kleckley	SC Electric & Gas Company	SERC	1
6.	Bob Jones	Southern Company Services	SERC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Pat Huntley	SERC Reliability Corp.	SERC 10										
8. Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 3, 5
2.	Eric Ervin	Westar Energy	SPP	1, 3, 5, 6
3.	Jonathan Hayes	Southwest Power Pool	SPP	2
4.	Bo Jones	Westar Energy	SPP	1, 3, 5, 6
5.	Tiffany Lake	Westar Energy	SPP	1, 3, 5, 6
6.	Stephen McGie	City of Coffeyville	SPP	NA
7.	Tracey Stewart	Southwestern Power Administration	SPP	1, 5
8.	Jamie Strickland	Oklahoma Gas & Electric	SPP	1, 3, 5
9.	Angela Summer	Southwestern Power Administration	SPP	1, 5

9.	Group	Jason Marshall	ACES Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bob Solomon	Hoosier Energy	RFC	1
2.	John Shaver	Arizona Electric Power Cooperative	WECC	4, 5
3.	John Shaver	Southwest Transmission Cooperative	WECC	1
4.	Amber Anderson	East Kentuck Power Cooperative	SERC	1, 3, 5
5.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT	1, 5
7.	Paul Jackson	Buckeye Power	RFC	3, 4
8.	Kevin Lyons	Central Iowa Power Cooperative	MRO	1

10.	Group	Albert DiCaprio	ISO/RTO Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Stephanie Monzon	PJM	RFC	2
2.	Bill Phillips	MISO	RFC	2
3.	Matt Goldberg	ISONE	NPCC	2
4.	Charles Yeung	SPP	SPP	2
5.	Steve Myers	ERCOT	ERCOT	2

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Greg Campoli	NYISO	NPCC 2										
7.	Ben Li	IESO	NPCC 2										
11.	Individual	Jana Van Ness, Director of Regulatory Compliance	Arizona Public Service Company	X		X		X	X				
12.	Individual	Emily Pennel	Southwest Power Pool Regional Entity										X
13.	Individual	Antonio Grayson	Southern Company	X		X		X	X				
14.	Individual	Thomas C. Duffy	Central Hudson Gas & Electric Corporation			X							
15.	Individual	David Ramkalawan	Ontario Power Generation					X					
16.	Individual	John Bee	Exelon	X		X	X	X	X				
17.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
18.	Individual	Andrew Z. Pusztai	American Transmission Company	X									
19.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
20.	Individual	David Jendras	Ameren	X		X		X	X				
21.	Individual	Patrick Brown	Essential Power, LLC					X					
22.	Individual	David Thorne	Pepco Holdings Inc.	X		X							
23.	Individual	Thad Ness	American Electric Power	X		X		X	X				
24.	Individual	Michelle D'Antuono	Occidental Energy Ventures Corp.			X		X		X			
25.	Individual	Patricia Metro	National Rural Electric Cooperative Association (NRECA)	X		X	X						
26.	Individual	Kathleen Goodman	ISO New England Inc.		X								
27.	Individual	Michael Falvo	Independent Electricity System Operator		X								
28.	Individual	Orlando Ciniglio	Idaho Power Company	X									
29.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				
30.	Individual	Jason Snodgrass	Georgia Transmission Corporation	X									
31.	Individual	Daniela Hammons	CenterPoint Energy	X									
32.	Individual	Oliver Burke	Entergy Services, Inc. (Transmission)	X									

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Summary Consideration: Thank you to Exelon and ISO New England, Inc. for supporting the comments of EEI and SRC, respectively. The Standard Drafting Team (SDT) will address the specific comments of SRC below, and notes that EEI did not submit specific comments.

Organization	Supporting Comments of "Entity Name"
Exelon	Exelon agrees with EEIs position and comments submitted related to this project.
ISO New England Inc.	ISO RTO Council Standards Review Committee (SRC)

1. If retired, do any Reliability Standard requirements proposed for retirement create a gap in reliability? If yes, please explain in the comment area.

Summary Consideration: In summary, no entity showed that a gap in reliability would result from the retirement of the proposed Reliability Standard requirements. Also, in general, the comments were very supportive of the retirement of the proposed Reliability Standard requirements, and the few questions or concerns raised are addressed in the individual responses. Based on comments and the recent approval of EOP-004-2 by the NERC Board of Trustees, CIP-001-2a R4 and EOP-004-1 R1 will be moved to Section V of the technical paper entitled: "The Initial Phase Reliability Standards Provided for Informational Purposes."

Organization	Yes or No	Question 1 Comment
ACES Standards Collaborators	No	(1) We do not see any reliability gaps created by the proposed retirements. Many of the requirements that have been moved to the second phase of the project could actually be retired in this phase without creating reliability gaps. We believe the approach to move several requirements to the second phase is overly conservative. However, we understand that drafting team must balance the retirement of requirements in this phase with satisfying concerns of stakeholders that no reliability gaps are created. (2) We are not opposed to the plan to review the linkages between BAL and INT standards in the next phase. However, we continue to believe that reloading of curtailed transactions is a commercial issue not a reliability issue. Thus, INT-004-2 easily meets criteria A and B and should be retired in phase one.
Response: ACES Standards Collaborators indicates that it did not see any reliability gaps resulting from the proposed Phase 1 retirement of requirements. The SDT acknowledges ACES Standards Collaborators' concern that deferring requirements to Phase 2 may be viewed as overly conservative, and the SDT notes that the requirements proposed in Phase 1 were influenced by the collaborative and expedited nature of Phase 1. The SDT also notes that it took just 5 months from the issuance of the Standards Authorization Request ("SAR") to a vote receiving over 90% approval for the Phase 1 requirements. In addition, on December 13, 2013, the Standards Committee passed a Reliability Standards Development Plan that requires the application of Paragraph 81		

Organization	Yes or No	Question 1 Comment
("P81") concepts to all new projects. One of the Reliability Standards Development Plan's projects is the review of the INT standards, including INT-004-2, which is scheduled to begin in the first quarter of 2013. Thus, the SDT believes that ACES Standards Collaborators' request for consideration of INT-004-2 will be timely and appropriately considered in the review of the INT standards, and, therefore, it is not necessary to include it in Phase 1 of P81.		
American Electric Power	No	AEP is not aware of any reliability gaps that would occur as a result of retiring the proposed Reliability Standards requirements.
Response: The SDT acknowledges AEP's comment that it is not aware of any reliability gaps resulting from the proposed Phase 1 retirement of requirements.		
CenterPoint Energy	No	CenterPoint Energy believes that the Reliability Standard requirements proposed for retirement in the initial phase ("Phase 1") of NERC Project 2013-02 'Paragraph 81' would not create a gap in reliability if they were retired. An increase in efficiency of the ERO compliance program should result with the removal of these Phase 1 requirements and the removal of additional Reliability Standard requirements in subsequent phases of this project.
Response: The SDT acknowledges CenterPoint Energy's comment that it believes that the proposed Phase 1 retirement of requirements should not create a gap in reliability and should also increase the efficiency of the ERO's compliance program.		
Occidental Energy Ventures Corp.	No	Occidental Energy Ventures Corp ("OEVC"). believes that the retirement of the Phase I requirements will pose little, if any, risk to the BES. However, in our view, this is a good start to a much more extensive restructuring of the regulatory model. Of course, the industry will need to gauge FERC's response to the initial grouping of requirements, but we should be prepared to aggressively push down this path.
Response: The SDT acknowledges Occidental Energy Ventures Corp's comment that it believes the proposed Phase 1 retirement of requirements will pose little, if any, risk to the Bulk Electric System, and its support for a more extensive restructuring of the regulatory model.		

Organization	Yes or No	Question 1 Comment
City of Austin dba Austin Energy	No	Please note: CIP-001-2a EA4 should be retired at the same time as CIP-001-2a R4 for the same reasons. We agree with the SDT regarding requirements applicable to the GO/GOP.
Response: During the balloting of the P81 Phase 1 requirements, EOP-004-2 was approved by stakeholders and the NERC Board of Trustees and was filed with its implementation plan on December 31, 2012 with regulatory agencies for approval. As part of the EOP-004-2 implementation plan, all of CIP-001-2a will be retired six months after regulatory approval. In the technical paper at Page 18, it was noted that: "… if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 project and may include CIP-001-2a R4 for informational purposes only." Given that a regulatory filing has been filed to retire all of CIP-001-2a, the SDT has revised the technical paper to include CIP-001-2a R4 for informational purposes only.		
Manitoba Hydro	No	Standard revision numbers and Requirement sequence changes should be made at a later date, as future revisions are required to each Standard that contains any retired Requirements. This will relieve the undesirable administrative burden, while reflecting accurate revision numbers and Requirement sequences, as changes are required to the Standards.
Response: The SDT agrees with Manitoba Hydro's comment that revisions to standard and requirement numbers should not be made at this time, given undesirable administrative burdens. The SDT has consulted with NERC staff on this issue, and no revision numbers will be implemented at this time.		
SERC EC Planning Standards Subcommittee	No	The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers"
Response: The SDT acknowledges that SERC EC Planning Standards subcommittee's comments are not the position of SERC Reliability Corporation.		

Organization	Yes or No	Question 1 Comment
Ontario Power Generation	No	The technical white paper has provided reasonable and well thought-out justifications for the retirement proposal to those reliability standard requirements.
Response: The SDT thanks Ontario Power Generation for its comment and agrees that the technical paper: "… has provided reasonable and well thought-out justifications for the retirement proposal to those reliability standard requirements."		
Southwest Power Pool Regional Entity	No	While CIP-007-3/4, Requirement R7.3 by itself has no immediate impact on the reliability of the Bulk Electric System, performance of R7.3 is required by the entity in order to be able to demonstrate compliance with CIP-007-3, Requirements R7.1 and R7.2 that, if not performed properly, could result in an impact to reliability. Elimination of this requirement could expose the registered entity to greater risk of non-compliance with the remaining requirements as it no longer requires the entity to maintain appropriate and sufficient evidence of performance with the remaining requirements. For the reasons described, the SPP RE is opposed to retiring CIP-007-3/4, Requirement R7.3.
Response: Southwest Power Pool Regional Entity states that while retirement of CIP-007-3, -4 R7.3: "… has no immediate impact on the reliability of the Bulk Electric System…" it is required to demonstrate compliance. As explained in the technical paper at Page 31, Section 400 of the NERC Rules of Procedure provides for a Regional Entity to request evidence to monitor compliance, and, therefore, it is unnecessary to also have a Reliability Standard that also requires the entity to retain records as set forth in CIP-007-3, -4 R7.3. The SDT also notes that the Responsible Entity has the burden to demonstrate compliance with CIP-007-3, -4 R7.1 and R7.2, notwithstanding the existence of CIP-007-3, -4 R7.3. For these reasons, the SDT affirms its decision to retire CIP-007-3, -4 R7.3.		
Northeast Power Coordinating Council	No	
Imperial Irrigation District (IID)	No	
Duke Energy	No	

Organization	Yes or No	Question 1 Comment
Bonneville Power Administration	No	
Dominion Resource Services	No	
Hydro One Networks Inc.	No	
SPP Standards Review Group	No	
Arizona Public Service Company	No	
Southern Company	No	
Central Hudson Gas & Electric Corporation	No	
American Transmission Company	No	
Ameren	No	
Essential Power, LLC	No	
Pepco Holdings Inc.	No	
National Rural Electric Cooperative Association (NRECA)	No	
Idaho Power Company	No	
Kansas City Power & Light	No	
Georgia Transmission Corporation	No	

Organization	Yes or No	Question 1 Comment
Entergy Services, Inc. (Transmission)	No	
Independent Electricity System Operator	Yes	1. BAL-005-0.2b, R2 - agree2. CIP-001-2a, R4 - we do not agree this is administrative in nature. Preparedness is an essential element in having the capability to readily respond to pressing reliability issues. Establishing contact with the enforcement authorities is a necessary component in preparing for reporting suspect or detected sabotage. Such reporting can help protect or minimize damages to BES facilities and/or Adverse Reliability Impact due to malicious acts. R1 to R3 do not have such a requirement to report sabotage events to the law enforcement authorities. If these authorities are included in Requirement R3, then the gap may be considered filled and R4 can be retired. However, this is not yet the case. We therefore suggest that R4 not be retired at this time.3. CIP-003-3, -4 R1.2 - agree4. CIP-003-3, -4 R3, R3.1, R3.2, R3.3 - while we agree that having the exception documented and approved by Senior Manager adds little to reliability, we do not agree that the entire requirement should be removed since this requirement is intended for implementing control of an entity's adherence to its Cyber Security policy, or document exceptions otherwise. Further, we do not concur with the SDT's view that over time, responsible entities may believe they can exempt themselves from compliance with the CIP requirements. Entities may exempt themselves from having some of their processes/procedures for cyber security not implemented, but their adherence to the policy and documenting exceptions are to be assessed during audit, which is not determined by the entities themselves. Any deviation from the requirement (the proposed "making exemption from compliance with the CIP requirement") will be identified and the entities will be found non-compliant. 5. CIP-003-3, -4 R4.2 - we agree that the action to classify the CCA information is redundant, but we do not think R4.2 can be removed entirely since the element "based on the sensitivity of the Critical Cyber Asset information" needs to be retained. Suggest to revise R4 to capture this element, or, at a minimum, consult the CIP SDT on the merit of retaining this element in R4.6. CIP-005-3a, -4a R2.6 -

Organization	Yes or No	Question 1 Comment
		agree.7. CIP-007-3, -4 R7.3 - agree.8. COM 001-1.1 R6 - agree.9. EOP-004-1 R1 - we do not agree with retiring this requirement. The RRO should have a formal reporting procedure in place to ensure adequate and detailed reporting is provided on system disturbances or any unusual event. This procedure is necessary for entities to meet the goals of further requirements in this standard that pertain to preliminary and final disturbance reporting .10. EOP-005-2 R3.1 - agree.11. EOP-009-0 R2 - agree.12. FAC-002-1 R2 - we do not agree that the requirement is burdensome. The requirement seems to meet the overarching criterion A from the White Paper (it requires responsible entities to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES), however, at a careful reading, the requirement seems to fail meeting at least one of the Criteria B: B1 (it is administrative, but not burdensome), B2 (it is data collection/retention, but we are not sure if NERC collects this data by any other method), B3 to B6 (it does not seem to fit any of these criteria).13. FAC-008-1 R1.3.5 - agree.14. FAC-008-1 R2; FAC-008-1 R3; FAC-008-3 R4; FAC-008-3 R5 - agree.15. FAC-010-2.1 R5; FAC-011-2 R5 - agree.16. FAC-013-2 R3 - agree.17. INT-007-1 R1.2 - agree, but there needs to be a requirement somewhere to stipulate that all entities involved in the Arranged Interchange must register with NERC such that transactions' participants can be contacted for confirmation of transactions being approved or to make changes when transactions are curtailed. Until such time that this requirement is developed elsewhere, INT-007-1 R1.2 should remain in effect. 18. IRO-016-1 R2 - It does not make sense to retire this requirement, but still keep M1 - the measure associated with requirement R1 - in the standard. M1 states that each RC must have evidence, such as operator log or another data source, of actions taken for the event or disagreement or both. However, R2 is the requirement which states the RC shall document the actions taken via operator log or another data source. Therefore, removing R2 would create inconsistency in the standard.19. NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4 we agree with retiring all of the 9.1, except R9.1.2: The agreement should contain the names of the applicable entities and the responsibilities assigned to

Organization	Yes or No	Question 1 Comment
		each one in relation to the NPIR.20. PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; PRC-010-0 R2; PRC-022-1 R2 - agree.21. TOP-001-1a R3 - agree.22. TOP-005-2a R1 - agree.23. VAR-001-2 R5 - agree.

Response: With respect to CIP-001-2a R4, Independent Electricity System Operator (IESO) expresses a concern that without R4, entities will not be properly prepared to contact law enforcement in the event of a sabotage event. During the comment and ballot period of the P81 project, EOP-004-2 was approved by stakeholders and the NERC Board of Trustees, and was filed with its implementation plan on December 31, 2012 with regulatory agencies for approval. As part of the EOP-004-2 implementation plan, all of CIP-001-2a will be retired six months after regulatory approval. In the technical paper at Page 18, it was noted that: "… if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 Project and may include CIP-001-2a R4 for informational purposes only." Given that a regulatory filing has been filed to retire all of CIP-001-2a, the SDT has revised the technical paper to include CIP-001-2a R4 for informational purposes only. For the same reasons, in response to IESO's concern on EOP-004-1 R1, the SDT has revised the discussion of EOP-004-1 R1 to include it in the technical paper for informational purposes only.

With respect to CIP-003-3, -4 R3, IESO believes that the entire requirement should not be removed because it is a control for adhering to the Cyber Security Policy. It also states that entities do not view CIP-003-3, -4 R3 and its sub-requirements as a way to exempt themselves from compliance with the Critical Infrastructure Protection (CIP) requirements. As stated in the technical paper at page 24, an entity has the ability to implement a Cyber Security Policy that exceeds the CIP requirements without the need for CIP-003-3, -4 R3 – which could also include implementing appropriate controls. The SDT does not find that retiring CIP-003-3, -4 R3 and its sub-requirements impacts the ability of an entity to implement appropriate controls to its Cyber Security Policy. Also, as stated in the technical paper at page 24, the SDT understands that the intent of CIP-003-3-, -4 R3 and its sub-requirements has been subject to misinterpretation, notwithstanding IESO's disagreement with the SDT on this matter. Therefore, the SDT affirms that CIP-003-3, -4 R3 and its sub-requirements should be retired.

In addition, IESO believes that the language in CIP-003-3, -4, R4.2 related to: "… based on the sensitivity of the Critical Cyber Asset information …" should be retained. In the technical paper at Page 26, it was explained that this language:

". . . requires the entity to develop classifications based on a subjective understanding of sensitivity (i.e., no clear connection to serving reliability) the requirement does not support reliability. In this context, classifying based on sensitivity becomes an

Organization	Yes or No	Question 1 Comment
administrative function that becomes necessarily burdensome because of all the possible ramifications 'based on sensitivity' can produce, and, therefore, require SMEs to decide on and reduce to writing in a documented program. This is time and effort that could be better spent on other CIP activities that provide value to cyber security and actively protect the BES." IESO has not presented sufficient rationale for the SDT to reconsider its decision as explained in the technical paper. Given the rationale in the technical paper on the lack of a nexus between the language "based on the sensitivity" and reliability, the SDT affirms its decision to retire CIP-003-3, -4 R.4.2. IESO does not agree that FAC-002-1 R2 is burdensome and while it seems to meet criterion A, it believes that the requirement fails to meet at least one of the Criteria B. As stated in the technical paper on Pages 40 and 41, FAC-002-1 R2 meets Criteria B1 (administrative) and B2 (data collection/retention) because it is an administrative documentation requirement and NERC and the Regional Entities have the authority under Section 400 of the NERC Rules of Procedure to require an entity to submit data and information for purposes of monitoring compliance. This would generally occur during a spot check or compliance audit where entities would already have the obligation to produce the information required in R2 to demonstrate compliance with R1 and its sub-requirements, even without the existence of R2. Therefore, the SDT affirms that FAC-002-1 R2 should be retired. IESO further believes that INT-007-1 R1.2 may not be retired until there is another requirement requiring entities involved in Arranged Interchange to register with NERC so that participants in those transactions can contact each other when transactions are curtailed. As explained in the technical paper at Pages 56 and 57, the North American Energy Standards Board has established registry and other rules related to entities entering into Arranged Interchange, and, therefore, INT-007-1 R1.2 is no longer necessary. Therefore, the SDT affirms its decision to retire INT-007-1 R1.2. IESO states that with the retirement of IRO-016-1 R2, Measure M1 should also be retired as it relates to R2. The SDT notes that Measure M1 was not retired because it identifies how to measure compliance with IRO-016-1 R1. IESO does not agree with retiring NUC-001-2 R9.1.2, stating that "… the agreement should contain the names of the applicable entities and the responsibilities assigned to each one in relation to the NPIR." Although the SDT understands the usefulness of an agreement stating who has responsibilities for the duties set forth in the agreement, as set forth in the technical paper at Page 61, this language is contractual boilerplate and has no direct nexus to reliability. Therefore, the SDT affirms its decision to retire NUC-001-2 R9.1.2.		
Exelon	Yes	Exelon believes that if a company takes an exception it should be documented

Organization	Yes or No	Question 1 Comment
		and proposes the following revision to R3: R3. Exceptions - Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented. R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
Response: Exelon prefers a modification to CIP-003-3, -4 R3 and the sub-requirements than retirement. As explained in the technical paper at Page 26, entities have the ability to develop its own procedures to take an exemption to its Cyber Security Policy in situations that it chooses to exceed the CIP requirements without the existence of CIP-003-3, -4 R3 and the sub-requirements. Thus, an entity has the flexibility to implement the revised exemption provision after the retirement of CIP-003-3, -4 R3 and the sub-requirements. Accordingly, the SDT affirms its decision to retire the CIP-003-3, -4 R3.		
ISO/RTO Standards Review Committee		The SRC has not identified any reliability gaps caused by the proposed actions, but the SRC believes that there is value in retaining some of the deleted requirements in some other form. Documentation is not an Operating or Assessment obligation but it is a unique topic Chain-of-command should be addressed as a Certification issue or as a Assumption / Definition Issue The following requirements while not appropriate as mandatory Reliability Standards should be retained in some category (highlighted text is a proposed category)BAL-005-0.2b R2 (Current Industry Operating Practice) CIP-003-3 R1.2 CIP-003-3 R3 CIP-003-3 R4.2 CIP-003-4 R3 CIP-003-4 R3.1 CIP-003-4 R3.2CIP-003-4 R3.3 CIP-003-4 R4.2 CIP-005-3a R2.6 CIP-005-4a R2.6 CIP-007-3 R7.3 CIP-007-4 R7.3 EOP-004-1 R1 (Industry Reports)EOP-005-2 R3.1 (Annual check-up / inspection)FAC-002-1 R2 ---FAC-008-1 R2 (Chain-of-Command)FAC-008-1 R3 ---FAC-008-3 R4 (Chain-of-Command)FAC-008-3 R5 ---FAC-010-2.1 R5** (Current Industry Assessment Practice)FAC-011-2 R5** (Current Industry Assessment Practice)FAC-013-2 R3 (Business Practice - NAESB)IRO-016-1 R2 (Documentation)NUC-001-2 R9.1 (Current Industry Operating Practice)NUC-001-2 R9.1.1 (Annual check-up / inspection)NUC-001-2 R9.1.2 (Documentation)NUC-001-2 R9.1.3 (Documentation)NUC-001-2 R9.1.4

Organization	Yes or No	Question 1 Comment
		(Certification)PRC-010-0 R2 (Current Industry Assessment Practice)PRC-022-1 R2 (Documentation)Please note the IESO will submit its own comments regarding the following requirements: CIP-001-2a R4CIP-003-3 R3.1 CIP-003-3 R3.2 CIP-003-3 R3.3 CIP-003-4 R14.2INT-007-1 R1.2 (Certification)VAR-001-2 R5** (Business Practice - NAESB)

Response: The SRC states that it does not see any reliability gap with the proposed retirements; however, it provides ideas on how some requirements may be useful in another format or forum. The SDT appreciates the SRC's ideas and encourages the SRC to work with the appropriate NERC committees to discuss and possibly implement its approach.

2. Do you have any comments on the technical white paper?

Summary Consideration: A few entities provided clarifying comments for consideration in the technical white paper, and those comments have been incorporated to enhance the readability and clarity of the technical white paper. A few commenters had concerns with the discussion of specific requirements and whether this was the time to renumber requirements; these concerns are addressed in the individual comments below. There were also comments related to possible formats for Phase 2, and while not within the scope of this SDT information, was provided based on the Standard Committee's approval of the Reliability Standards Developmental Plan. A few commenters also expressed concerns that were compliance related. The SDT reminds stakeholder that the focus of the P81 effort was to retire requirements that had little or no benefit to reliability.

Organization	Yes or No	Question 2 Comment
SERC EC Planning Standards Subcommittee	No	The comments expressed herein represent a consensus of the views of the above-named members of the SERC EC Planning Standards Subcommittee only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers"
Response: The SDT acknowledges that SERC EC Planning Standards subcommittee's comments are not the position of SERC Reliability Corporation.		
Northeast Power Coordinating Council	No	
Imperial Irrigation District (IID)	No	
Dominion Resource Services	No	
Arizona Public Service Company	No	

Organization	Yes or No	Question 2 Comment
Ontario Power Generation	No	
Exelon	No	
American Transmission Company	No	
Ameren	No	
Essential Power, LLC	No	
American Electric Power	No	
Independent Electricity System Operator	No	
Idaho Power Company	No	
Kansas City Power & Light	No	
CenterPoint Energy	No	
Entergy Services, Inc. (Transmission)	No	
Pepco Holdings Inc.	Yes	As part of this effort, a new revision number for any standard that is changed should be used. Also any measurements or registered entities (e.g. RRO) that would no longer apply should be deleted.

Response: The SDT agrees with Pepco Holdings that measurements associated with retired requirements should be concurrently retired. The SDT points Pepco Holdings to the posted redline of the Reliability Standards that retires measurements associated with retired requirements. For administrative efficiency, the Reliability Standards will not be renumbered and functional entities will not be deleted at this time, but the next time the standard is revised it is understood that renumbering and removal of

Organization	Yes or No	Question 2 Comment
entities that are no longer applicable will occur.		
ACES Standards Collaborators	Yes	(1) On page 5, several requirements are marked with two asterisks but there is no footnote or additional information. Please indicate the purpose of the asterisks or remove them. (2) The supporting statement in the technical whitepaper and SAR that Criteria C is needed to make an informed decision "in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B" is inconsistent with the actual Criteria. Criterion C2 questions if the requirement is being reviewed in an on-going standards development project. While this is certainly a relevant question and a valid reason to not include a requirement in the P81 project, the question simply provides no input on whether Criteria A and B are met. We suggest changing the supporting statement to be clearer that Criteria C in essence is more information to make an informed decision but may not necessarily have any indication on whether Criteria A and B are satisfied. (3) The supporting statement in the technical whitepaper and SAR that Criteria C provides "additional information to assist in the determination of whether a Reliability Standard requirement satisfies both Criteria A and B" is inconsistent with the SAR. In the detailed description, the SAR states that the initial phase shall only identify requirements that satisfy both Criteria A and B. These are supposed to be the requirements that easily meet these two criteria sets. Thus, why is Criteria C evaluated in the whitepaper. If these criteria are easily met, Criteria C is not needed to assist in the determination and the associated information while interesting would appear to be superfluous.
Response: ACES Standards Collaborators seeks clarification of the use of ** on Page 5 of the technical white paper. The SDT refers ACES Standards Collaborators to Footnote 4 of the technical white paper that states: "Those requirements that were not part of the draft SAR, but were added based on stakeholder comments are denoted by a '' throughout this technical white paper."** **ACES Standards Collaborators also seeks clarification on the role of Criteria C. The SDT notes that Criteria C was only considered after a requirement met both Criteria A and B. The application of Criteria C provided additional information that in some cases**		

Organization	Yes or No	Question 2 Comment
emphasized the need to retire the requirement (*e.g.,* was not results-based) and other times indicated that it may not be necessary to continue with retirement (*e.g.,* the requirement was already scheduled in a reasonable period of time to be retired through another standards project). The SDT believes this approach is consistent with the clarification sought by ACES Standards Collaborators, and, thus will clarify the language in the technical white paper on the application of Criteria C. The SDT also notes that the SAR states that, "…for all phases, the standard drafting team shall also consider the data and reference points set forth below in Criterion C when deciding whether a Reliability Standard requirement should be retired or modified."		
Bonneville Power Administration	Yes	BPA appreciates the drafting team's decision to include TOP-001-1 R3 in the technical white paper for informational purposes rather than proposing to retire it.
Response: The SDT is appreciative of Bonneville Power Administration's understanding of the treatment of TOP-001-1 R3.		
Central Hudson Gas & Electric Corporation	Yes	CHG&E believes the reason for retiring CIP-003-3,-4 R3 and its sub-requirements is fallacious. The reason provided in the technical white paper is essentially: " First, and most importantly, that requirement has never been available for use to exempt an entity form compliance with any requirement of any NERC reliability standard. It only applies to exceptions to internal corporate policy, and only in cases where the policy exceeds a NERC standard requirement, or addresses an issue that is not covered in a NERC reliability standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of 8 characters in length, and be changed every 30 days, this provision could be used for internal governance purposes to lessen the corporate requirement, back to the password requirements in CIP-007 R5.3, or in conjunction with a TFE to something else. The removal of this requirement has no effect on the TFE process, or compliance with any other NERC reliability standard requirement."CHG&E wishes to highlight the fact that NERC has no jurisdiction to impose or grant exceptions to internal corporate policies. Therefore, this requirement (and its sub - requirements) can only have been crafted to address exceptions to the NERC CIP requirements. Throughout this standard, the NERC requirements for a 'cyber security policy' are delineated. This requirement specifically addresses exceptions

Organization	Yes or No	Question 2 Comment
		to the 'cyber security policy'. As written, this requirement can only be interpreted to mean that an exception to the NERC CIP required 'cyber security policy' is acceptable if properly documented and approved by the CIP Senior Manager. Central Hudson Gas & Electric Corporation strongly disagrees with the inclusion of CIP-003-3, -4 Requirements R3, R3.1, R3.2, R3.3 as candidates for retirement. The reasons stated in the SAR in favor of inclusion are that these requirements are administrative in nature and are purely examples of a documentation process. Further it is stated in the SAR that they, ".... have been subject to misinterpretation, including responsible entities believing they can exempt themselves from compliance with the CIP requirements." This last statement is precisely the reason why the aforementioned requirements were included in the standard. These requirements allow Registered Entities to, on rare occasions, take an exception to one or several of the CIP requirements (for a limited period of time) if they (1) have valid cause (major emergency, Force Majeure, etc.), (2) document the occurrence and (3) are reviewed and approved by the CIP Senior Manager. This process supports the Registered Entity's compliance effort and acknowledges the need for special protocols to address emergency circumstances. Without such a process, the only recourse for the Registered Entity is to self-report a violation which is not within their control. In other words, retirement of these requirements would force the Registered Entity to be in full compliance with ALL CIP Standards ALL the time regardless of circumstance. The concept of realistic expectations was undoubtedly the reason these requirements were crafted and included in the standard. Further, with regard to the Registered Entity's decision to claim an exception, a system of checks and balances already exists. At the time of a compliance audit of the standard's requirements, the Regional Entity reviews and makes a determination as to whether the actions taken by the Registered Entity were warranted. Further, the fact that this requirement is included in the FFT process is of little consolation since any exception would still constitute a violation of the NERC Standard on the part of the Registered Entity and would carry with that violation the associated stakeholder

Organization	Yes or No	Question 2 Comment
		liability.
Response: CHG&E disagrees with retiring CIP-003-3,-4 R3 and its sub-requirements. CHG&E is concerned that the language in the technical white paper on CIP-003-3,-4 R3 and its sub-requirements could be interpreted as NERC having jurisdiction to impose or grant exceptions to internal corporate policies and would require that entities be in compliance with all CIP requirements all of the time regardless of the circumstance and with no avenue to take an exemption to the CIP requirements. On the former point, the SDT clarifies that it was not the intent of the language in the technical white paper on CIP-003-3,-4 R3 and its sub-requirements to opine on the jurisdiction of NERC over "internal corporate policies." With respect to CHG&E's latter concern, it appears more compliance-related than reliability-based. The criteria set forth in the SAR and technical white paper are focused on impacts to reliability, not compliance. The SDT believes CHG&E's compliance concerns are more appropriately discussed with its Regional Entity's or NERC's compliance and enforcement monitoring staff. For informational purposes only, the SDT points to the language in CIP-003-3, -4 R1.1 "… including provision for emergency situations …" and R2.4 "The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy" as language CHG&E may wish to consider in light of its concerns." In addition, in R1 there is a requirement to "document and implement" a Cyber Security policy which at a *minimum* must contain the following: "… addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations." In discussing this with the CIP SDT leadership, it was their intent in developing this requirement to allow entities to only waive the portions of those implemented policies which were in excess of the CIP-002-3 through CIP-009-3 set of requirements. In other words, NERC and FERC would not approve this R3 requirement if it allowed waiving other requirements by simply documenting an exception. The SDT finds no reason presented by CHG&E that indicates that it should reverse its decision to retire CIP-003-3,-4 R3 and its sub-requirements. Thus, the SDT affirms its decision to retire CIP-003-3,-4 R3 and its sub-requirements.		
Manitoba Hydro	Yes	CIP-003-3,-4 R1.2: Technical Justification (page 19): CIP personnel should act based on their cyber security policy; a policy which must address the CIP-002 through CIP-009 standards as required by CIP-003 R1.1. As a result, the specific training processes and procedures will reflect the cyber security policy. We suggest "they will act via their specific training, processes and procedures which reflect the overarching cyber security policy." CIP-007-3, -4 R7.3: (1) Technical Justification (page 32): For added clarity, we suggest the wording "... small number of Reliability Standard requirements explicitly mandating ....". (2) Data and information collection for ERO compliance monitoring purposes is certainly within

Organization	Yes or No	Question 2 Comment
		the context of the Reliability Standards. For added clarity, we suggest the wording "... for ERO compliance monitoring purposes without specific data collection language in the Reliability Standards." (3) It is unclear who "the entities" are. Should this state "Responsible Entities"? (4) For additional clarity, we suggest the wording "... the Reliability Standards are arguably more difficult to understand ...".
Response: The SDT appreciates Manitoba Hydro suggested enhancements and has worked them into the technical white paper. The SDT also notes that the term Responsible Entities is defined as "entities" on Page 6 of the technical white paper.		
Southern Company	Yes	FAC-002-1 R2-The comments in the technical white paper concerning FAC-002-1 R2 are correct. Entities already have the obligation to provide the documentation of the evaluation of the reliability impact of new facilities upon request to demonstrate compliance to R1 and its sub-requirements, thus making R2 unnecessary. Furthermore, a requirement to retain documentation does not benefit or protect the reliable operation of the BES.VAR-001-2 R5: While Southern agrees that the elimination of VAR-001-2, R5 is appropriate, there is some concern that the justification that the TOP's adherence to R2 as a double check to ensure there are sufficient reactive power resources to protect the voltage levels under normal and Contingency conditions may be viewed by FERC as redirecting the burden from the PSEs and LSEs to the TOP. The LSE's (particularly) need to make their reactive resources available to the TOP in order for the TOP to acquire/use these reactive resources to protect voltage levels. Also, consider that not all entities necessarily take service under a transmission tariff, so references to other contractual mechanisms such as Interchange Agreements, etc. might be cited in the Technical White Paper for ensuring sufficient reactive resources are provided and made available by transmission customers.
Response: The SDT agrees with the clarifications suggested by Southern Company and has worked them into the technical paper.		
Georgia Transmission Corporation	Yes	GTC is very supportive of the recent ERO, Regional Entity and industry stakeholder efforts in response to the opportunity provided by FERC in paragraph 81 of the

Organization	Yes or No	Question 2 Comment
		Find, Fix, Track and Report Order to review and eliminate standards that provide no or minimal reliability benefits. However, we are disappointed with the small number of requirements that are proposed for retirement in this initial phase of work. GTC would like to note that because duplicative requirements for subsequent versions of Reliability Standards are never mandatory at the same time, the net impact of requirements being proposed for retirement identified in the "Redline of Standards with Proposed Retirements" for phase 1 is only 28 out of 1650 FERC approved requirements or 1.7%. This small percentage does not seem to reflect well on the view that NERC's FFT initiative is predicated on, of which FERC has extended an invitation to justify without imposing a deadline. From our review of the P81 Technical White Paper, it appears that there are many more requirements in addition to the 28 identified that meet the criteria for deletion. And while a phased approach has been recommended, the certainty associated with subsequent phases occurring in a timely manner is questionable and GTC recommends a big picture approach. We believe the small number of requirements identified in phase I would be more palatable if a big picture perspective was provided once submitting to FERC. For example, a breakdown similar to the one below would provide more confidence that future phases would occur and be successful: o At the end of the day, we believe we can eliminate approximately xx number or xx percentage of requirements o This will be completed in three phases o Phase one will include approximately xx requirements, posted to FERC in fourth quarter, 2012 o Phase two will include approximately xx requirements, posted to FERC in xx quarter, 2013 o Phase three posting will...Laying out the bigger picture keeps the momentum going and also let's FERC know that the first posting only begins to scratch the surface of the issue. Furthermore, we are aware of current standards drafting teams that are drafting requirements that would meet the criteria for deletion stated in this Technical White Paper. There is a pressing need to implement a mechanism to ensure "P81-qualified" requirements are not drafted going forward or eliminated prior to NERC BOT approval.GTC will continue to support this effort as it moves through the NERC standards development process and participate in future phases

Organization	Yes or No	Question 2 Comment
		of work related to the P81 project. Our goal is to ensure future phases of this effort lead to retirement of a much greater number of requirements that are not necessary for the reliability of the BES.
Response: Georgia Transmission Corporation raises points related to whether Phase 1 of P81 included sufficient requirements and the uncertainty and the timing of subsequent phases. As noted above, the Standards Committee recently approved a Reliability Standards Development Plan that requires P81 concepts to be applied to all Standard projects. Training will be offered to SDTs to ensure no new requirements would be introduced that might contradict this effort. The SDT is also encouraged that the Reliability Standards Development Plan has set forth an aggressive schedule to review the entire set of standards in 2013, many of which were identified by stakeholders in response to the draft P81 SAR.		
Hydro One Networks Inc.	Yes	Hydro One very much appreciates the efforts of the SDT in trying to streamline and focus current standards to focus on requirement that impact to reliability. In addition to this, we hope that:- Phase II of this project will continue along the same path and advance the approach to other approved standards, and- Work on new and reviewed standards will include the criteria developed in this project (i.e. SDTs are fully directed to use Paragraph 81 criteria while developing new and reviewing existing standards).
Response: As noted above, the Standards Committee recently approved a Reliability Standards Development Plan that requires P81 concepts to be applied to all standard projects. The SDT is also encouraged that the Reliability Standards Development Plan has set forth an aggressive schedule to review the entire set of standards in 2013, many of which were identified by stakeholders in response to the draft P81 SAR. Thus, the SDT is hopeful that the recent approval of the Reliability Standards Development Plan will help continue on the Phase 1 path as recommended by Hydro One Networks Inc.		
National Rural Electric Cooperative Association (NRECA)	Yes	NRECA is very supportive of the recent ERO, Regional Entities and industry stakeholder efforts in response to the opportunity provided by FERC in P81 of the Find, Fix, Track and Report Order to review and eliminate standard requirements that provide no or minimal reliability benefits. NRECA is disappointed with the small number of requirements that are proposed for retirement in this initial phase of work, but will support this effort as it moves through the NERC standards

Organization	Yes or No	Question 2 Comment
		development process and will continue participating in future phases of work related to the P81 project. It is our goal to ensure future phases of this effort lead to retirement of a much greater number of requirements that are not necessary for the reliability of the Bulk Electric System. NRECA has reviewed the P81 Technical White Paper. It appears that there are many more requirements, in addition to the 38 identified, that meet the criteria for deletion most of which were included in the SAR for this project. Although the phase approach to this project was explained and many of the requirements included in the SAR will be addressed in a subsequent phases of the project, there is a concern that the future phases of the project will not be completed in a timely manner since there is no timeline provided for the future phases in the Implementation Plan for this project. Having such a time-line will demonstrate to the FERC that the industry and the ERO are dedicated to eliminating standard requirements that provide no or minimal reliability benefits. NRECA is concerned that drafting teams are drafting requirements that would meet the criteria for deletion stated in this Technical White Paper. There must be a mechanism in place to ensure "P81-qualified" requirements are not included in standards that are under development or in standards that are provided to the NERC BOT for approval. In addition, if requirements are retired that include an entity that is only required to comply with the standard because of the specific requirement that is to be retired said entity should be removed from the applicability of the standard. An example of such is VAR-01, R5 where this requirement is the only requirement applicable to a PSE, but the PSE has not been removed from the Applicability of the standard in the red-line version posted for comment.
Response: Similar to our response to Georgia Transmission Corporation and Hydro One Networks Inc, the SDT hopes that the recent approval of the Reliability Standards Development Plan will help to alleviate any concerns of National Rural Electric Cooperative Association on the timing and content of Phase 2, as the Reliability Standards Development Plan requires P81 concepts to be applied to all standard projects. Training will also be offered to SDTs to ensure no new requirements would be introduced that might contradict this effort. The SDT also notes that the issue identified related to removing the PSE from the applicability section of VAR-001 will occur the next time that standard is reviewed and re-numbered, which based on the		

Organization	Yes or No	Question 2 Comment
Reliability Standards Developmental Plan, is scheduled for 2013.		
Occidental Energy Ventures Corp.	Yes	OEVC believes the drafting team did an excellent job researching and defending each proposed retirement. In our view, this is a fundamental necessity as we must assume that FERC will closely scrutinize each one. However, we anticipate that some form of cost/benefit analysis will be requested in each case - particularly since the entire impetus behind the Paragraph 81 project is the shortage of compliance resources. It may be a worthwhile exercise to develop a cost model that accounts for industry and CEA resources accurately and effectively. The results must be weighed against the expected benefit of any requirement - as the industry and regulatory bodies clearly have some important trade-offs to consider. In particular, with FERC's recent emphasis on cyber security, cold weather preparation, and geomagnetic protection, some of the less effective requirements need to be removed. OEVC believes that the Commission will be reluctant to proceed in this manner without data that demonstrates the comparative benefit of each requirement.
Response: Occidental Energy Ventures Corp. suggests that the SDT consider using a cost benefit analysis or exercise that accounts for industry and CEA resources. The SDT notes that the Standards Committee has approved a cost effectiveness analysis process ("CEAP") and will be implementing a pilot of this process on two standards projects in the first half of 2013. At this time, cost effectiveness considerations are not sufficiently developed to be applicable to the requirements proposed in Phase 1, nor does P81 express an expectation that such analysis for this project would be undertaken, and is focused on deletion of requirements that do little or nothing to contribute to reliability. Thus, while the SDT will not apply a cost effective test to the requirements proposed for retirement, the SDT suggests that Occidental Energy Ventures Corp. follow the developments on the CEAP Project as posted on the NERC "Standards Under Development" webpage through the Standards Committee.		
SPP Standards Review Group	Yes	Page 17 - The 6th through 12th lines are a stretch and do not add anything to the argument for retiring Requirement 3 of CIP-001-2a. It is conjecture on the part of the drafting team and should be removed from the paper. If the drafting team doesn't agree and keeps this portion, please insert the word 'require' between 'some' and 'corporate' in the 8th line. Also, delete 'to generic' in the 11th line.

Organization	Yes or No	Question 2 Comment
		Page 26 - In the 10th line of the Technical Justification paragraph, insert 'task' between 'administrative' and 'that'. Page 29 - At the beginning of the 6th line of the Technical Justification paragraph, delete the 'is'. Page 32 - In the first line of the Criterion A paragraph, insert a 'not' between 'does' and 'promote'. Page 59 - In the 8th line of the 2nd paragraph, the sentence 'Thus, IRO-016-1 R1 does not support reliability.' doesn't seem right. Shouldn't this be; it does support reliability? Or perhaps you meant to say that R2 does not support reliability. Also, in the next sentence, delete the second 'that'. Page 61 - In the 15th line of the Technical Justification paragraph, delete the 'an' in front of unnecessarily.
Response: SPP Standards Review Group suggests that the SDT remove CIP-001-2a R4 from the technical paper. As noted above, this requirement is already proposed for retirement through EOP-004-2, and, therefore, will be included in the technical paper for informational purposes only. **The SDT appreciates SPP Standards Review Group's suggestions to improve the readability of the technical paper and have made the suggested changes.**		
City of Austin dba Austin Energy	Yes	Please note: CIP-001-2a EA4 should be retired at the same time as CIP-001-2a R4 for the same reasons. We agree with the SDT regarding requirements applicable to the GO/GOP.
Response: Please see response to the City of Austin's comments to question 1.		
ISO/RTO Standards Review Committee	Yes	The SRC agrees with the removal of the identified requirements. The SRC recognizes that the scope of this SAR is to identify inappropriate requirements and not necessarily to suggest what to do with those identified requirements for removal. The SRC suggests that the Technical White Paper recognize that some of these removed requirements can and should be retained (just not retained as Reliability Standards). See response to Q1 for suggestions.

Organization	Yes or No	Question 2 Comment
Response: Please see the SDT's response to the SRC's comments to question 1.		
Southwest Power Pool Regional Entity	Yes	The white paper discussion for CIP-007-3/4, Requirement R7.3 proffers the idea that most data and information is collected for ERO compliance monitoring purposes outside of the context of Reliability Standards. While this might be the case of other standards, the SPP RE does not believe this is the case for the CIP-002 through CIP-009 Cyber Security standards, collectively referred to as the "CIP standards." The CIP standards require the entity to produce a document (e.g., policy, program, procedure, process, or list); to implement a documented program, process, or procedure; and/or to perform and document certain measurable procedural steps. In the absence of disposition records, which are specifically not required by CIP-007-3/4, Requirements R7.1 and R7.2, there will unlikely be any data or information outside of the context of the Reliability Standards demonstrating compliance with R7.1 and R7.2. The authors of the white paper appear to object to the maintenance of process documentation in this instance yet do not object to other requirements in the CIP standards that similarly call for the production and maintenance of documentation. The SPP RE is concerned that the authors of the white paper have chosen to focus on individual requirements in a stand-alone manner and have failed to understand the supportive interrelationships of the CIP standards and their requirements.
Response: Southwest Power Pool Regional Entity states that data and information related to CIP requirements are collected through the CIP requirements. Southwest Power Pool Regional Entity is particularly concerned that with the "… absence of disposition records, which are specifically not required by CIP-007-3/4, Requirements R7.1 and R7.2, there will unlikely be any data or information outside of the context of the Reliability Standards demonstrating compliance with R7.1 and R7.2." As explained above, Section 400 of the NERC Rules of Procedure provides Regional Entities with the authority to request information needed to monitor compliance and the Responsible Entity has the burden of proof to demonstrate compliance. As stated in the technical white paper at Pages 31 and 32, there is no direct nexus between data retention and reliability. This is a compliance issue that is better served through procedures promulgated outside of the Reliability Standards. Thus, the SDT affirms its decision to retire CIP-007-3, -4 R7.3.		

Organization	Yes or No	Question 2 Comment
Southwest Power Pool Regional Entity also generally questions whether the SDT understands the interrelationship between the CIP requirements, because other CIP data retention requirements are not proposed for retirement in Phase 1. The SDT notes that the number and type of CIP requirements proposed for retirement in Phase 1 was shaped to some degree by the collaborative process between stakeholders and the staffs of the Regional Entities and NERC. The SDT also collaborated with the leadership of the CIP V5 SDT on the CIP requirements proposed for retirement. The SDT's evaluations and discussions confirmed the appropriateness to retire the proposed CIP requirements. That is not to say, there are not other CIP data retention requirements that should be considered for retirement in the future. Thus, while the SDT understands Southwest Power Pool Regional Entity's concern, it affirms its decision to retire the selected CIP requirements in Phase 1.		
Duke Energy	Yes	While we agree with retiring all of the Reliability Standard requirements proposed for retirement, we believe the P81 Project Technical White Paper should be more forceful in justifying retirement of the CIP requirements. Specifically, the "not an important part of a scheme of CIP Requirements" phrase is often used in Criteria C sections discussing VFR and AML issues. It would seem that FERC may have difficulty giving this phrase credibility since (i) the industry previously had balloted to approve such requirements, (ii) NERC BOT approved such requirements, and (iii) FERC approved such requirements. All of these approvals seem to indicate that all such entities previously believed that the requirements were important to the CIP scheme. Instead, we suggest that this phrase be replaced in each instance with phrases like the following: "As explained above and since the inception of this requirement, this requirement has not been shown to constitute a [key][integral] part of a scheme of CIP requirements."
Response: The SDT appreciates Duke Energy's suggestions to clarify the technical white paper. The SDT believes that the intent of the language in the technical white paper is consistent with the suggestions of Duke Energy.		

END OF REPORT

A. Introduction

1. **Title:** **Automatic Generation Control**

2. **Number:** BAL-005-0.2b

3. **Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.

4. **Applicability:**

   4.1. Balancing Authorities

   4.2. Generator Operators

   4.3. Transmission Operators

   4.4. Load Serving Entities

5. **Effective Date:** May 13, 2009

B. Requirements

R1. All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.

R1.1. Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.

R1.2. Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.

R1.3. Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retired)

R3. A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.

R4. A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.

R5. A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.

R6. The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

R7. The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.

R8. The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.

R8.1. Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.

R9. The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.

R9.1. Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.

R10. The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.

R11. Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.

R12. Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.

R12.1. Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.

R12.2. Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.

R12.3. Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.

R13. Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.

R14. The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.

R15. The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

R16. The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

1.1.1. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.

1.1.2. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

1.3.1. Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.

1.3.2. Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Effective Date: August 27, 2008 (U.S.)

Interpretation of BAL-005-0 Automatic Generation Control, R17

Request for Clarification received from PGE on July 31, 2007

PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

BAL-005-0

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25% of full scale
Remote terminal unit	≤ 0.25% of full scale
Potential transformer	≤ 0.30% of full scale
Current transformer	≤ 0.50% of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to "annually check and calibrate" does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to "annually check and calibrate" the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system

operator. Frequency inputs from other sources that are for reference only are excluded. The time error and frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-3

3. Purpose: Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-003-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-3 Requirement R2.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

	3	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within thirty calendar days of the effective date.	
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3. (Retired)	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1. (Retired)	LOWER	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
R3.2. (Retired)	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3. (Retired)	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	The Responsible Entity has established but not documented a change	The Responsible Entity has established but not documented both a change control process and configuration management	The Responsible Entity has not established and documented a change control process OR	The Responsible Entity has not established and documented a change control process AND

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		control process OR The Responsible Entity has established but not documented a configuration management process.	process.	The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a configuration management process.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-3a

3. Purpose: Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability

4.1. Within the text of Standard CIP-005-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-3, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-3 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity	

		shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation
3a	02/02/11	Approved by FERC	
3a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal

Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	and Standard CIP-009-4.	and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter.		
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6. (Retired)	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.			
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to designated response personnel.	Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	Revised.
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"
4a	4/19/12	FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3a, 4a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

3. Purpose: Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-007-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-3 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical)	

		Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
3	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, **but did not document** that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).

		testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).		
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.
R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program **but** did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.

R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.

R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
R5.1.1.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

			manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).		
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 **but** did not maintain records as specified in R7.3. (Retired)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A
R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3. (Retired)	LOWER	N/A	N/A	N/A	N/A

Formatted: Font color: Red

R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A
R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

E. **Regional Variances**

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Restoration from Blackstart Resources**

2. Number: EOP-005-2

3. Purpose: Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

4. Applicability:

4.1. Transmission Operators.

4.2. Generator Operators.

4.3. Transmission Owners identified in the Transmission Operators restoration plan.

4.4. Distribution Providers identified in the Transmission Operators restoration plan.

5. Proposed Effective Date: Twenty-four months after the first day of the first calendar quarter following applicable regulatory approval. In those jurisdictions where no regulatory approval is required, all requirements go into effect twenty-four months after Board of Trustees adoption.

B. Requirements

R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Time Horizon = Operations Planning]*

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

R1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

R1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.

R2. Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. *[Time Horizon = Operations Planning]*

R3. Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule. *[Time Horizon = Operations Planning]*

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary. (Retired)

R4. Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan. *[Time Horizon = Operations Planning]*

R4.1. Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.

R5. Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date. *[Time Horizon = Operations Planning]*

R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify: *[Time Horizon = Long-term Planning]*

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

R7. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each

affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration. *[Time Horizon = Real-time Operations]*

R8. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator. *[Time Horizon = Real-time Operations]*

R9. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Time Horizon = Operations Planning]*

R9.1. The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

R9.2. A list of required tests including:

R9.2.1. The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.

R9.2.2. The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

R9.3. The minimum duration of each of the required tests.

R10. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following: *[Time Horizon = Operations Planning]*

R10.1. System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.

R10.2. Restoration priorities.

R10.3. Building of cranking paths.

R10.4. Synchronizing (re-energized sections of the System).

R11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks. *[Time Horizon = Operations Planning]*

R12. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Time Horizon = Operations Planning]*

R13. Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. *[Time Horizon = Operations Planning]*

R14. Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. *[Time Horizon = Operations Planning]*

R15. Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator's restoration plan within 24 hours following such change. *[Time Horizon = Operations Planning]*

R16. Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. *[Time Horizon = Operations Planning]*

R16.1. Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R9.

R16.2. Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.

R17. Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: *[Time Horizon = Operations Planning]*

R17.1. System restoration plan including coordination with the Transmission Operator.

R17.2. The procedures documented in Requirement R14.

R18. Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator. *[Time Horizon = Operations Planning]*

C. Measures

M1. Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator.

M2. Each Transmission Operator shall have evidence such as e-mails with receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan in accordance with Requirement R2.

M3. Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, e-mails with receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.

M4. Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, e-mails with receipts, or registered mail receipts, that it has updated its restoration plan and submitted it to its Reliability Coordinator in accordance with Requirement R4.

M5. Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan available in its primary and backup control rooms and its System Operators prior to its implementation date in accordance with Requirement R5.

M6. Each Transmission Operator shall have documentation such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.

M7. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved shall have evidence such as voice recordings, e-mail, dated computer printouts, or operator logs, that it implemented its restoration plan or restoration plan strategies in accordance with Requirement R7.

M8. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved in such an event shall have evidence, such as voice recordings, e-mail, dated computer printouts, or operator logs, that it resynchronized shut down areas in accordance with Requirement R8.

M9. Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R9.

M10. Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R10.

M11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R11.

M12. Each Transmission Operator shall have evidence, such as training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R12.

M13. Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R13.

M14. Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R14.

M15. Each Generator Operator with a Blackstart Resource shall provide evidence, such as e-mails with receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within twenty-four hours of such changes in accordance with Requirement R15.

M16. Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R16.

M17. Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R17.

M18. Each Generator Operator shall have evidence, such as dated training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R18.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Approved restoration plan and any restoration plans in force since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of an updated restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three years for Requirement R4, Measure M4.
- The current, restoration plan approved by the Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- Implementation of its restoration plan or restoration plan strategies on any occasion for three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R7, Measure M7.
- Resynchronization of shut down areas on any occasion over three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R8, Measure M8.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R9, Measure M9.
- Actual training program materials or descriptions for three calendar years for Requirement R10, Measure M10.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit as well as one previous compliance audit period for Requirement R12, Measure M12.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator, applicable Transmission Owner, and applicable Distribution provider shall keep data or evidence to show compliance as identified

below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Actual training program materials or descriptions and actual training records for three calendar years for Requirement R11, Measure M11.

If a Transmission Operator, applicable Transmission owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in force since its last compliance audit for Requirement R13, Measure M13.

The Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current documentation and any documentation in force since its last compliance audit on procedures to start each Blackstart Resources and for energizing a bus for Requirement R14, Measure M14.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R15, Measure M15.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R16, Measure M16.
- Actual training program materials and actual training records for three calendar years for Requirement R17, Measure M17.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Generator Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R18, Measure M18.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	May 2, 2007	Approved by Board of Trustees	Revised
2	TBD	Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-005-2 (approval effective 5/23/11)	
2	TBD	R3.1 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Coordination of Plans For New Generation, Transmission, and End-User Facilities

2. Number: FAC-002-1

3. Purpose: To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.

4. Applicability:

4.1. Generator Owner

4.2. Transmission Owner

4.3. Distribution Provider

4.4. Load-Serving Entity

4.5. Transmission Planner

4.6. Planning Authority

5. (Proposed) Effective Date: The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:

1.1. Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.

1.2. Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.

1.3. Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.

1.4. Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.

1.5. Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected

transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days). (Retired)

C. Measures

M1. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider's documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.

M2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Timeframe

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting

Complaints

1.4. Data Retention

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

1.5. Additional Compliance Information

None

2. Violation Severity Levels (no changes)

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata
1	TBD	Modified to address Order No. 693 Directives contained in paragraph 693.	Revised.

1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Facility Ratings Methodology**

2. Number: FAC-008-1

3. Purpose: To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Transmission Owner

4.2. Generator Owner

5. Effective Date: August 7, 2006

B. Requirements

R1. The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:

R1.1. A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R1.2. The method by which the Rating (of major BES equipment that comprises a Facility) is determined.

R1.2.1. The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

R1.2.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R1.3. Consideration of the following:

R1.3.1. Ratings provided by equipment manufacturers.

R1.3.2. Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).

R1.3.3. Ambient conditions.

R1.3.4. Operating limitations.

R1.3.5. Other assumptions.

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request. (Retired)

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the

Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

C. Measures

M1. The Transmission Owner and Generator Owner shall each have a documented Facility Ratings Methodology that includes all of the items identified in FAC-008 Requirement 1.1 through FAC-008 Requirement 1.3.5.

M2. The Transmission Owner and Generator Owner shall each have evidence it made its Facility Ratings Methodology available for inspection within 15 business days of a request as follows: (Retired)

M2.1 The Reliability Coordinator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Reliability Coordinator Area. (Retired)

M2.2 The Transmission Operator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its portion of the Reliability Coordinator Area. (Retired)

M2.3 The Transmission Planner shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Transmission Planning Area. (Retired)

M2.4 The Planning Authority shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Planning Authority Area. (Retired)

M3. If the Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall have evidence that it provided a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Transmission Owner and Generator Owner shall self-certify its compliance to the Compliance Monitor at least once every three years. New Transmission Owners and Generator Owners shall each demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

The Transmission Owner and Generator Owner shall each keep all superseded portions of its Facility Ratings Methodology for 12 months beyond the date of the change in that methodology and shall keep all documented comments on the Facility Ratings Methodology and associated responses for three years. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant.

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Transmission Owner and Generator Owner shall each make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 Facility Ratings Methodology

1.4.2 Superseded portions of its Facility Ratings Methodology that had been replaced, changed or revised within the past 12 months

1.4.3 Documented comments provided by a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Authority on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology, and the associated responses

2. Levels of Non-Compliance

2.1. Level 1: There shall be a level one non-compliance if any of the following conditions exists:

2.1.1 The Facility Ratings Methodology does not contain a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.1.2 The Facility Ratings Methodology does not address one of the required equipment types identified in FAC-008 R1.2.1.

2.1.3 No evidence of responses to a Reliability Coordinator's, Transmission Operator, Transmission Planner, or Planning Authority's comments on the Facility Ratings Methodology. (Retired)

2.2. Level 2: The Facility Ratings Methodology is missing the assumptions used to determine Facility Ratings or does not address two of the required equipment types identified in FAC-008 R1.2.1.

2.3. Level 3: The Facility Ratings Methodology does not address three of the required equipment types identified in FAC-008-1 R1.2.1.

2.4. Level 4: The Facility Ratings Methodology does not address both Normal and Emergency Ratings ~~or the Facility Ratings Methodology was not made available for inspection within 15 business days of receipt of a request~~. (Deleted text retired)

Formatted: Strikethrough

E. **Regional Differences**

None Identified.

Version History

Version	Date	Action	Change Tracking
1	01/01/05	1. Lower cased the word "draft" and "drafting team" where appropriate. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Changed "Timeframe" to "Time	01/20/05

		Frame" and "twelve" to "12" in item D, 1.2.	
1	TBD	R2 and R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Facility Ratings**

2. **Number:** FAC-008-3

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.

4. **Applicability**

   4.1. Transmission Owner.

   4.2. Generator Owner.

5. **Effective Date:** The first day of the first calendar quarter that is twelve months beyond the date approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter twelve months following BOT adoption.

B. Requirements

R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:

- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
- Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:

2.2.1. Equipment Rating standard(s) used in development of this methodology.

2.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

2.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

2.2.4. Operating limitations.[1]

2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.4. The process by which the Rating of equipment that comprises a Facility is determined.

2.4.1. The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

2.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R3. Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

3.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:

3.2.1. Equipment Rating standard(s) used in development of this methodology.

[1] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

3.2.4. Operating limitations.[2]

3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

3.4. The process by which the Rating of equipment that comprises a Facility is determined.

3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R7. Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

[2] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

8.1. As scheduled by the requesting entities:

8.1.1. Facility Ratings

8.1.2. Identity of the most limiting equipment of the Facilities

8.2. Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1. Identity of the existing next most limiting equipment of the Facility

8.2.2. The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

C. Measures

M1. Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.

M2. Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.

M3. Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.

M4. Each Transmission Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement 4. The Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its documentation for determining its Facility Ratings or its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement R4. (Retired)

M5. If the Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology or a Generator Owner's documentation for determining its Facility Ratings, the Transmission Owner or Generator Owner shall have evidence, (such as a copy of a dated electronic or hard copy note, or other comparable evidence from the Transmission Owner or Generator Owner addressed to the commenter that includes the response to the comment,) that it provided a response to that commenting entity in accordance with Requirement R5. (Retired)

M6. Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).

M7. Each Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R7.

M8. Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability

Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority**

Regional Entity

1.2. **Compliance Monitoring and Enforcement Processes:**

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting
- Compliance Violation Investigations
- Complaints

1.3. **Data Retention**

The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.

The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.

The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.

The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.

The Generator Owner and Transmission Owner shall each keep evidence for Measure M4, and Measure M5, for three calendar years. (Retired)

The Generator Owner shall keep evidence for Measure M7 for three calendar years.

The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.

If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. **Additional Compliance Information**

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	• The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part 2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
R3	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	• 3.2.2 • 3.2.3 • 3.2.4	• 3.2.2 • 3.2.3 • 3.2.4	OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
R4 (Retired)	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.	The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.	The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)
R5 (Retired)	The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)	The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)	The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation. (R5)	The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
R7	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the requesting entities.
R8	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1)	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more

Formatted Table

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)	than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)

Formatted Table

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	
3	TBD	R4 and R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Standard FAC-010-2.1 — System Operating Limits Methodology for the Planning Horizon

A. Introduction

1. Title: **System Operating Limits Methodology for the Planning Horizon**

2. Number: FAC-010-2.1

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable planning of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Planning Authority

5. Effective Date: April 19, 2010

B. Requirements

R1. The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the planning horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R2.5. Starting with all Facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.6. In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:

R2.6.1. Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers.

R3. The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).

R3.2. Selection of applicable Contingencies.

R3.3. Level of detail of system models used to determine SOLs.

R3.4. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.5. Anticipated transmission system configuration, generation dispatch and Load level.

R3.6. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.

R4. The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:

R4.1. Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.

R4.2. Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.

R4.3. Each Transmission Planner that works in the Planning Authority's Planning Authority Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. Measures

M1. The Planning Authority's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Planning Authority shall have evidence it issued its SOL Methodology and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Planning Authority that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Planning Authority shall self-certify its compliance to the Compliance Monitor at least once every three years. New Planning Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Planning Authority shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

Formatted: Strikethrough

Formatted: Font color: Red

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Planning Authority shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology. (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R2.1 through R2.3 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.2	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
R2	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 –R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
R3	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
R4	One or both of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority failed to issue its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but

Requirement	Lower	Moderate	High	Severe
				four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
R5 (Retired)	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

E. **Regional Differences**

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-010.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
1	November 1, 2006	Fixed typo. Removed the word "each" from the 1st sentence of section D.1.3, Data Retention.	01/11/07
2	June 24, 2008	Adopted by Board of Trustees; FERC Order 705	Revised
2		Changed the effective date to July 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2.1	November 5, 2009	Adopted by the Board of Trustees — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	April 19, 2010	FERC Approved — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Operating Limits Methodology for the Operations Horizon**

2. Number: FAC-011-2

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: April 29, 2009

B. Requirements

R1. The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the operations horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. In determining the system's response to a single Contingency, the following shall be acceptable:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in FAC-011 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. Interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies

R2.3.3. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R3. The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)

R3.2. Selection of applicable Contingencies

R3.3. A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.

R3.3.1. This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies.

R3.4. Level of detail of system models used to determine SOLs.

R3.5. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.6. Anticipated transmission system configuration, generation dispatch and Load level

R3.7. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_V.

R4. The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:

R4.1. Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.

R4.2. Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.

R4.3. Each Transmission Operator that operates in the Reliability Coordinator Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. **Measures**

M1. The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Reliability Coordinator that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5 (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

Formatted: Strikethrough

Formatted: Font color: Red

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R3.1, R3.2, R3.4 through R3.7 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.1, R3.2, R3.4 through R3.7.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4.

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
R4	One or both of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to

Requirement	Lower	Moderate	High	Severe
				30 calendar days after the effectiveness of the change.
R5 (Retired)	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

2. Number: FAC-013-2

3. Purpose: To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.

4. Applicability:

4.1. Planning Coordinators

5. Effective Date:

In those jurisdictions where regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after applicable regulatory approval or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-2 are effective.

In those jurisdictions where no regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after Board of Trustees adoption or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1 and MOD-030-2 are effective.

B. Requirements

R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Criteria for the selection of the transfers to be assessed.

1.2. A statement that the assessment shall respect known System Operating Limits (SOLs).

1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's planning practices.

1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:

1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.

1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.

1.4.3. System demand.

1.4.4. Current approved and projected Transmission uses.

1.4.5. Parallel path (loop flow) adjustments.

1.4.6. Contingencies

1.4.7. Monitored Facilities.

1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.

R2. Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. Distribute to the following prior to the effectiveness of such revisions:

2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.

2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.

2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]* (Retired)

R4. During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

R5. Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

R6. If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

C. Measures

M1. Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.

M2. Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2

M3. Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. (Retired)

M4. Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.

M5. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5.

M6. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Data Retention

The Planning Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. (R3 retired)
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.

Formatted Table

Formatted Table

R2	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.
R3 **(Retired)**	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.

R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.

Formatted Table

R5	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.

Formatted Table

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	08/01/05	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Lower cased the word "draft" and "drafting team" where appropriate. 3. Changed Anticipated Action #5, page 1, from "30-day" to "Thirty-day." 4. Added or removed "periods."	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	5/17/12	FERC Order issued directing the VRF's for Requirements R1. and R4. be changed from "Lower" to "Medium." FERC Order issued correcting the High and Severe VSL language for R1.	
2	TBD	R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Interchange Confirmation**

2. Number: **INT-007-1**

3. Purpose: To ensure that each Arranged Interchange is checked for reliability before it is implemented.

4. Applicability

4.1. Interchange Authority.

5. Effective Date: January 1, 2007

B. Requirements

R1. The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:

R1.1. Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry. (Retired)

R1.3. The following are defined:

R1.3.1. Generation source and load sink.

R1.3.2. Megawatt profile.

R1.3.3. Ramp start and stop times.

R1.3.4. Interchange duration.

R1.4. Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.

C. Measures

M1. For each Arranged Interchange, the Interchange Authority shall show evidence that it has verified the Arranged Interchange information prior to the dissemination of the Confirmed Interchange.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Time Frame

The Performance-Reset Period shall be twelve months from the last noncompliance to Requirement 1.

1.3. Data Retention

The Interchange Authority shall keep 90 days of historical data. The Compliance Monitor shall keep audit records for a minimum of three calendar years.

1.4. Additional Compliance Information

Each Interchange Authority shall demonstrate compliance to the Compliance Monitor within the first year that this standard becomes effective or the first year the entity commences operation by self-certification to the Compliance Monitor.

Subsequent to the initial compliance review, compliance may be:

1.4.1 Verified by audit at least once every three years.

1.4.2 Verified by spot checks in years between audits.

1.4.3 Verified by annual audits of noncompliant Interchange Authorities, until compliance is demonstrated.

1.4.4 Verified at any time as the result of a complaint. Complaints must be lodged within 60 days of the incident. Complaints will be evaluated by the Compliance Monitor.

Each Interchange Authority shall make the following available for inspection by the Compliance Monitor upon request:

1.4.5 For compliance audits and spot checks, relevant data and system log records for the audit period which indicate an Interchange Authority's verification that all Arranged Interchange was balanced and valid as defined in R1. The Compliance Monitor may request up to a three-month period of historical data ending with the date the request is received by the Interchange Authority.

1.4.6 For specific complaints, only those data and system log records associated with the specific Interchange event contained in the complaint which indicate an Interchange Authority's verification that an Arranged Interchange was balanced and valid as defined in R1 for that specific Interchange

2. Levels of Non-Compliance

2.1. Level 1: One occurrence[1] where Interchange-related data was not verified as defined in R1.

2.2. Level 2: Two occurrences where Interchange-related data was not verified as defined in R1.

2.3. Level 3: Three occurrences where Interchange-related data was not verified as defined in R1.

2.4. Level 4: Four or more occurrences where Interchange-related data was not verified as defined in R1.

E. Regional Differences

None

[1] This does not include instances of not verifying due to extenuating circumstances approved by the Compliance Monitor.

Version History

Version	Date	Action	Change Tracking
1	TBD	R1.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Coordination of Real-time Activities Between Reliability Coordinators**

2. Number: **IRO-016-1**

3. Purpose: To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: November 1, 2006

B. Requirements

R1. The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.

R1.1. If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.

R1.2. If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).

R1.2.1. If time permits, this re-evaluation shall be done before taking corrective actions.

R1.2.2. If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

R1.3. If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both. (Retired)

C. Measures

M1. For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

The performance reset period shall be one calendar year.

1.3. Data Retention

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

1.4. Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction's discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

2. Levels of Non-Compliance

2.1. Level 1: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
Version 1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Hyphenated "30-day" and "Reliability Coordinator-to-Reliability Coordinator" when used as adjective.	01/20/06

		3. Changed standard header to be consistent with standard "Title." 4. Added "periods" to items where appropriate. 5. Initial capped heading "Definitions of Terms Used in Standard." 6. Changed "Timeframe" to "Time Frame" in item D, 1.2. 7. Lower cased all words that are not "defined" terms — drafting team, and self-certification. 8. Changed apostrophes to "smart" symbols. 9. Removed comma after word "condition" in item R.1.1. 10. Added comma after word "expected" in item 1.4, last sentence. 11. Removed extra spaces between words where appropriate.	
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Nuclear Plant Interface Coordination**

2. Number: NUC-001-2

3. Purpose: This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. Applicability:

4.1. Nuclear Plant Generator Operator.

4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

4.2.1 Transmission Operators.

4.2.2 Transmission Owners.

4.2.3 Transmission Planners.

4.2.4 Transmission Service Providers.

4.2.5 Balancing Authorities.

4.2.6 Reliability Coordinators.

4.2.7 Planning Coordinators.

4.2.8 Distribution Providers.

4.2.9 Load-serving Entities.

4.2.10 Generator Owners.

4.2.11 Generator Operators.

5. Effective Date: April 1, 2010

B. Requirements

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Medium*]

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

R4.1. Incorporate the NPIRs into their operating analyses of the electric system.

R4.2. Operate the electric system to meet the NPIRs.

R4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

R5. The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]

R9.1. Administrative elements: (Retired)

R9.1.1. Definitions of key terms used in the agreement. (Retired)

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. (Retired)

R9.1.3. A requirement to review the agreement(s) at least every three years. (Retired)

R9.1.4. A dispute resolution mechanism. (Retired)

R9.2. Technical requirements and analysis:

R9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

R9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

R9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

R9.3. Operations and maintenance coordination:

R9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

R9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

R9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

R9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

R9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. .

R9.3.6. Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

R9.3.7. Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

R9.4. Communications and training:

R9.4.1. Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

R9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

R9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

R9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

R9.4.5. Provisions for personnel training, as related to NPIRs.

C. Measures

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. (Requirement 2 and 9)

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:

M4.1 The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)

M4.2 The electric system was operated to meet the NPIRs. (Requirement 4.2)

M4.3 The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)

M8. The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

2.1. Lower: Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.

2.2. Moderate: Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.

2.3. High: One or more requirements of R3 through R8 were not met.

2.4. Severe: No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

E. Regional Differences

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs.
Therefore the definition of NPLR for Canadian CANDU units will be as follows:

Nuclear Plant Licensing Requirements (NPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	Revision
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update
2	TBD	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.**

2. Number: PRC-010-0

3. Purpose: Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.

4. Applicability:

4.1. Load-Serving Entity that operates a UVLS program

4.2. Transmission Owner that owns a UVLS program

4.3. Transmission Operator that operates a UVLS program

4.4. Distribution Provider that owns or operates a UVLS program

5. Effective Date: April 1, 2005

B. Requirements

R1. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).

R1.1. This assessment shall include, but is not limited to:

R1.1.1. Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.

R1.1.2. Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.

R1.1.3. A review of the voltage set points and timing.

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). (Retired)

C. Measures

M1. Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0_R1.

M2. Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

1.2. Compliance Monitoring Period and Reset Timeframe

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0_R1.1 or an assessment of the UVLS program was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

A. Introduction

1. **Title:** **Under-Voltage Load Shedding Program Performance**

2. **Number:** **PRC-022-1**

3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).

4. **Applicability**

   4.1. Transmission Operator that operates a UVLS program.

   4.2. Distribution Provider that operates a UVLS program.

   4.3. Load-Serving Entity that operates a UVLS program.

5. **Effective Date:** May 1, 2006

B. Requirements

R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UVLS set points and tripping times.

R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.

R1.4. A summary of the findings.

R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. (Retired)

C. Measures

M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.

M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization. (Retired)

D. Compliance

1. Compliance Monitoring Process

   1.1. Compliance Monitoring Responsibility

   Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

2.3. Level 3: Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

2.4. Level 4: Documentation of the analysis of UVLS performance was not provided.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	December 1, 2005	1. Removed comma after 2004 in "Development Steps Completed," #1. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Lower cased the word "region," "board," and "regional" throughout document where appropriate. 4. Added or removed "periods" where appropriate. 5. Changed "Timeframe" to "Time Frame" in item D, 1.2.	January 20, 2006
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Voltage and Reactive Control**

2. **Number:** VAR-001-2

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators.

   4.2. Purchasing-Selling Entities.

   4.3. Load Serving Entities.

5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.

R2. Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

R3. The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.

R3.1. Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.

R3.2. For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.

R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule [1] at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider. (Retired)

[1] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

R6. The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.

R6.1. When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.

R7. The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.

R8. Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.

R9. Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to support its voltage under first Contingency conditions.

R9.1. Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.

R10. Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.

R11. After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

R12. The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

C. Measures

M1. The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule as specified in Requirement 4 to each Generator Operator it requires to follow such a schedule.

M2. The Transmission Operator shall have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3.2.

M3. The Transmission Operator shall have evidence to show that it issued directives as specified in Requirement 6.1 when notified by a Generator Operator of the loss of an automatic voltage regulator control.

M4. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with Requirement 11.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months.

The Compliance Monitor shall retain any audit data for three years.

1.5. Additional Compliance Information

The Transmission Operator shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Violation Severity Levels (no changes)

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	TBD	Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised.
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan
Project 2013-02 – Paragraph 81

Requested Approvals

- None

Requested Retirements

- BAL-005-0.2b R2
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3
- CIP-003-3 R4.2
- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2
- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-1 R2
- FAC-008-1 R3
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5
- FAC-011-2 R5
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5

Note that when these Requirements are retired, the version numbers of the standards will NOT be incremented, but the retired Requirements and associated elements will be clearly marked as retired. After evaluating the options and consulting with the Standards Committee and Standards Committee Process Subcommittee, the P81 drafting team determined that this was the most practical approach. Incrementing the version numbers of each standard is impractical because, in some cases, a subsequent version has already been developed. In addition, incrementing the version would require renumbering Requirements where a retired Requirement created a gap in numbering, and this creates an undesirable administrative burden for entities using certain systems to manage their compliance programs.

Prerequisite Approvals

- None

Revisions to Defined Terms in the NERC Glossary

- None

Background

On September 30, 2011, the North American Electric Reliability Corporation (NERC) filed a petition with the Federal Energy Regulatory Commission (FERC) requesting approval of its proposal to make informational filings in a "Find, Fix, Track and Report" (FFT) spreadsheet of lesser-risk, remediated possible violations of Reliability Standards. On March 15, 2012, the FERC issued an order conditionally accepting NERC's FFT proposal. In paragraph 81 (P81) of that order, the FERC stated:

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently. North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, a draft Standards Authorization Request (SAR) was drafted to set forth criteria and a process to identify Reliability Standard requirements that either: (a) provide little protection to the Bulk Electric System; (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file to retire the identified Reliability Standard requirements with appropriate governmental authorities.

Standards Process Input Group (SPIG)

In addition to addressing P81, the SAR was drafted consistent with what the SPIG developed as Recommendation No. 4, as set forth in NERC's Recommendations to Improve The Standards Development Process on page 12 (April 2012), which states:

> Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

Collaborative Process

The draft SAR and a suggested list of Reliability Standard requirements embedded in the SAR for consideration in the Initial Phase was the product of collaborative discussions among the following entities and their members: Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group. The draft SAR was posted for comment, which were due September 4, 2012. The P81 Standards Drafting Team reviewed the comments and finalized the SAR and the proposed list of Reliability Standard requirements for retirement.

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Authority
- Load Serving Entity
- NERC
- Planning Authority
- Planning Coordinator
- Purchasing-Selling Entity
- Regional Entity
- Regional Reliability Organization
- Reliability Coordinator
- Transmission Service Provider
- Transmission Operator
- Transmission Owner
- Transmission Planner

Effective Date of Retirements

All of the Requirements will be retired on the day of approval by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter after approval by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Note that no complete standard is being proposed for retirement and all of the other Requirements in each of the affected standards will remain in continuous effect.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan
Project 2013-02 – Paragraph 81

Requested Approvals

- None

Requested Retirements

- BAL-005-0.2b R2
- ~~CIP-001-2a R4~~
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3
- CIP-003-3 R4.2
- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2
- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- ~~EOP-004-1 R1~~
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-1 R2
- FAC-008-1 R3
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5
- FAC-011-2 R5
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5

Note that when these Requirements are retired, the version numbers of the standards will NOT be incremented, but the retired Requirements and associated elements will be clearly marked as retired. After evaluating the options and consulting with the Standards Committee and Standards Committee Process Subcommittee, the P81 drafting team determined that this was the most practical approach. Incrementing the version numbers of each standard is impractical because, in some cases, a subsequent version has already been developed. In addition, incrementing the version would require renumbering Requirements where a retired Requirement created a gap in numbering, and this creates an undesirable administrative burden for entities using certain systems to manage their compliance programs.

Prerequisite Approvals

- None

Revisions to Defined Terms in the NERC Glossary

- None

Background

On September 30, 2011, the North American Electric Reliability Corporation (NERC) filed a petition with the Federal Energy Regulatory Commission (FERC) requesting approval of its proposal to make informational filings in a "Find, Fix, Track and Report" (FFT) spreadsheet of lesser-risk, remediated possible violations of Reliability Standards. On March 15, 2012, the FERC issued an order conditionally accepting NERC's FFT proposal. In paragraph 81 (P81) of that order, the FERC stated:

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently. North American Electric Reliability Corporation, 138 FERC ¶ 61,193 at p 81 (March 15, 2012) ("P81").

Consistent with P81, a draft Standards Authorization Request (SAR) was drafted to set forth criteria and a process to identify Reliability Standard requirements that either: (a) provide little protection to the Bulk Electric System; (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file to retire the identified Reliability Standard requirements with ~~FERC to have them removed from the FERC-approved list of Reliability Standards~~appropriate governmental authorities.

Standards Process Input Group (SPIG)

In addition to addressing P81, the ~~draft~~ SAR was drafted consistent with what the SPIG developed as Recommendation No. 4, as set forth in NERC's Recommendations to Improve The Standards Development Process on page 12 (April 2012), which states:

> Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

Collaborative Process

The draft SAR and a suggested list of Reliability Standard requirements embedded in the SAR for consideration in the Initial Phase was the product of collaborative discussions among the following entities and their members: Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, Transmission Access Policy Study Group, the North American Electric Reliability Corporation, and the Regional Entity Management Group. The draft SAR was posted for comment, which were due September 4, 2012. The P81 Standards Drafting Team reviewed the comments and finalized the SAR and the proposed list of Reliability Standard requirements for retirement.

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Authority
- Load Serving Entity
- NERC
- Planning Authority
- Planning Coordinator
- Purchasing-Selling Entity
- Regional Entity
- Regional Reliability Organization
- Reliability Coordinator
- Transmission Service Provider
- Transmission Operator
- Transmission Owner
- Transmission Planner

Effective Date of Retirements

All of the Requirements will be retired on the day of approval by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter after approval~~ed~~ by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Note that no complete standard is being proposed for retirement and all of the other Requirements in each of the affected standards will remain in continuous effect ~~until such time that the entire standard may be retired~~.

Paragraph 81 Project Technical White Paper

December 20, 2012

Table of Contents

P81 Project Technical White Paper

December 20, 2012

I. Introduction

On March 15, 2012, the Federal Energy Regulatory Commission ("FERC" or Commission") issued an order[1] on the North American Electric Reliability Corporation's ("NERC") Find, Fix and Track ("FFT") process that stated in paragraph 81 ("P81"):

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the [Electric Reliability Organization] ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

A. Consensus Process

In response to P81 and the Commission's request for comments to be coordinated,[2] during June and July 2012, various industry stakeholders, Trade Associations,[3] staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria,

---

[1] *North American Electric Reliability Corporation,* 138 FERC ¶ 61,193 at P 81 (2012).

[2] In addition to addressing P81, the consensus effort was also consistent with recommendation #4 set forth in *NERC's Recommendations to Improve The Standards Development Process* at page 12 (April 2012), which states:

Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

[3] Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, and Transmission Access Policy Study Group.

and, thus, could be retired. Specifically, the three parties (industry stakeholders/Trade Associations, staff from NERC, and staff from the NERC Regions) used the following conservative discipline to arrive at the proposed list of requirements to be retired: (i) the development of criteria to determine whether a Reliability Standard requirement should be retired and (ii) the application of this criteria with consultation from Subject Matter Experts ("SME"), with the understanding that if any of the three parties objected to including a requirement it would not be included in the initial phase of the P81 Project. As a result of this process, a draft Standards Authorization Request ("SAR"), including an initial suggested list of requirements for retirement, was drafted and presented to the NERC Standards Committee. Also, the SMEs consulted in this process provided the technical justifications that appear in this technical white paper.

B. Standards Committee

On July 11, 2012, the Standards Committee authorized the draft SAR to be posted for industry comment and formed an interim P81 Standards Drafting Team ("SDT") to review and respond to comments as well as finalize the SAR. The draft SAR was posted on August 3, 2012 with stakeholder comments due on or before September 4, 2012. Based on the stakeholder comments received, the SDT finalized the SAR, including the criteria and the initial list of Reliability Standard requirements proposed for retirement. On September 28, 2012, the Standards Committee Executive Committee authorized: (a) waiving the 30 day initial comment period and (b) posting the SAR and list of requirements proposed for retirement in the initial phase for a 45-day formal comment period with the formation of a ballot pool during the first 30 days and an initial ballot during the last 10 days of that 45-day comment period.[4]

The purpose of this technical white paper is to set forth the background and technical justification for each of the Reliability Standard requirements proposed for retirement. Stakeholders are requested to review this technical white paper and provide the SDT any: (1) supplemental, additional technical justifications for a requirement(s) and/or (2) concerns with the technical justifications for a requirement(s).

[4] The following requirements that were presented in the draft SAR were already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the Board in November), and, thus, are presented in this technical white paper in Section V for informational purposes only: CIP-001-2a R4; COM-001-1.1 R6; EOP-004-1 R1; EOP-009-0 R2; FAC-008-1 R1.3.5; PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; TOP-001-1a R3; and TOP-005-2a R1. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the Board of Trustees for retirement or filed with the Commission or Canadian governmental authorities as part of the P81 Project. Those requirements that were not part of the draft SAR, but were added based on stakeholder comments are denoted by a "**" throughout this technical white paper. More detail on each of these requirements is provided below.

II. Executive Summary

The SDT developed a set of three criteria and used them to identify requirements that could be eligible for retirement. A summary of the criteria are as follows:

A. Criterion A (Overarching Criterion): little, if any, benefit or protection to the reliable operation of the BES

B. Criteria B (Identifying Criteria)
   - B1. Administrative
   - B2. Data Collection/Data Retention
   - B3. Documentation
   - B4. Reporting
   - B5. Periodic Updates
   - B6. Commercial or Business Practice
   - B7. Redundant

C. Criteria C (Additional data and reference points)
   - C1. Part of a FFT filing
   - C2. Being reviewed in an ongoing Standards Development Project
   - C3. Violation Risk Factor ("VRF") of the requirement
   - C4. Tier in the 2013 Actively Monitored List ("AML")
   - C5. Negative impact on NERC's reliability principles
   - C6. Negative impact on the defense in depth protection of the BES
   - C7. Promotion of results or performance based Reliability Standards

Specifically, for a requirement to be proposed for retirement, it must satisfy both, Criterion A and at least one of the Criteria B. Criteria C were considered as additional information to make a more informed decision.

Based on the criteria above, the SDT proposes to retire the following 36 requirements in 23 Reliability Standard versions:

- BAL-005-0.2b R2
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3
- CIP-003-3 R4.2

- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2
- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-1 R2
- FAC-008-1 R3
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5**
- FAC-011-2 R5**
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5**

A table is included in Appendix A with the Reliability Standard requirements proposed for retirement and a cross-reference to the associated criteria.

III. Criteria

The P81 Project focuses on identifying FERC-approved Reliability Standard requirements that satisfy the criteria set forth below.[5] Specifically, for a Reliability Standard requirement to be proposed for retirement it must satisfy **both**: (i) Criterion A

[5] The scope of future phases of the P81 Project has not yet been determined. When the scope is considered, the criteria set forth herein may be a useful guide to appropriate criteria for those phases.

(the overarching criterion) and (ii) at least one of the Criteria B listed below (identifying criteria). The purpose of having these two levels of criteria was to confine the review and consideration of requirements to only those requirements that clearly need not be included in the mandatory Reliability Standards. Also, Criteria A and B were designed so there would be no rewriting or consolidation of requirements, and the technical merits of retiring the requirements did not require significant research and vetting. In addition, for each Reliability Standard requirement proposed for retirement, the data and reference points set forth below in Criteria C were considered to make a more informed decision on whether to proceed with retirement. Lastly, for each requirement proposed for retirement, any increase to the efficiency of the ERO compliance program is addressed.

Criterion A (Overarching Criterion)

The Reliability Standard requirement requires responsible entities ("entities") to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Section 215(a) (4) of the United States Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

Criteria B (Identifying Criteria)

B1. Administrative

The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

This criterion is designed to identify requirements that can be removed with little effect on reliability and whose removal will result in an increase in the efficiency of the ERO compliance program. Administrative functions may include a task that is or is not related to developing procedures or plans, such as establishing communication contacts. Thus, for certain requirements, Criterion B1 is closely related to Criteria B2, B3 and B4. Strictly administrative functions do not inherently negatively impact reliability directly and, where possible, should be eliminated for purposes of efficiency and to allow the ERO and entities to appropriately allocate resources.

B2. Data Collection/Data Retention

These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

This criterion is designed to identify requirements that can be removed with little effect on reliability. The collection and/or retention of data do not necessarily have a reliability benefit and yet are often required to demonstrate compliance. Where data collection and/or data retention is unnecessary for reliability purposes, such requirements should be eliminated in order to increase the efficiency of the ERO compliance program.

B3. Documentation

The Reliability Standard requirement requires responsible entities to develop a document (*e.g.*, plan, policy or procedure) which is not necessary to protect BES reliability.

This criterion is designed to identify requirements that require the development of a document that is unrelated to reliability or has no performance or results-based function. In other words, the document is required, but no execution of a reliability activity or task is associated with or required by the document.

B4. Reporting

The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there would be little reliability impact.

B5. Periodic Updates

The Reliability Standard requirement requires responsible entities to periodically update (*e.g.*, annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

This criterion is designed to identify requirements that impose an updating requirement that is out of sync with the actual operations of the BES, unnecessary or duplicative.

B6. Commercial or Business Practice

The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

This criterion is designed to identify those requirements that require: (i) implementing a best or outdated business practice or (ii) implicating the exchange of or debate on commercially sensitive information while doing little, if anything, to promote the reliable operation of the BES.

B7. Redundant

The Reliability Standard requirement is redundant with: (i) another FERC-approved Reliability Standard requirement(s); (ii) the ERO compliance and monitoring program or

(iii) a governmental regulation (*e.g.*, Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

This criterion is designed to identify requirements that are redundant with other requirements and are, therefore, unnecessary. Unlike the other criteria listed in Criterion B, in the case of redundancy, the task or activity itself may contribute to a reliable BES, but it is not necessary to have two duplicative requirements on the same or similar task or activity. Such requirements can be removed with little or no effect on reliability and removal will result in an increase in efficiency of the ERO compliance program.

Criteria C (Additional data and reference points)

To assist in the determination of whether to proceed with the requirement of a Reliability Standard requirement that satisfies both Criteria A and B, the following data and reference points shall be considered to make a more informed decision:

C1. Was the Reliability Standard requirement part of a FFT filing?

The application of this criterion involves determining whether the requirement was included in a FFT filing.

C2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?

The application of this criterion involves determining whether the requirement proposed for retirement is part of an active on-going Standards Development Project, with a consideration of the point in the process that Project is at. If the requirement has been passed by the stakeholders and is scheduled to be presented to the NERC Board of Trustees, in most cases it will not be included in the P81 project to promote regulatory efficiency. The exception would be a requirement, such as the Critical Information Protection ("CIP") requirements for Version 3 and 4, that is not due to be retired for an extended period of time; or, other requirements that based on the specific facts and circumstances of that requirement indicate it should be retired via the P81 Project first rather than waiting for another Standards Development Project to retire it, particularly as a way to increase the efficiencies of the ERO compliance program. Also, for informational purposes, whether the requirement is included in a future or pending Standards Development Project will be identified and discussed.

C3. What is the VRF of the Reliability Standard requirement?

The application of this criterion involves identifying the VRF of the requirement proposed for retirement, with particular consideration of any requirement that has been assigned as having a Medium or High VRF. Also, the fact that a requirement has a

Lower VRF is not dispositive that it qualifies for retirement. In this regard, Criterion C3 is considered in light of Criterion C5 (Reliability Principles) and C6 (Defense in Depth) to ensure that no reliability gap would be created by the retirement of the Lower VRF requirement. For example, no requirement, including a Lower VRF requirement, should be retired if its retirement harms the effectiveness of a larger scheme of requirements that are purposely designed to protect the reliable operation of the BES.

C4. In which tier of the 2013 AML does the Reliability Standard requirement fall?

The application of this criterion involves identifying whether the requirement proposed for retirement is on the 2013 AML, with particular consideration for any requirement in the first tier of the 2013 AML.

C5. Is there a possible negative impact on NERC's published and posted reliability principles?

The application of this criterion involves consideration of the eight following reliability principles published on the NERC webpage.

> **Reliability Principles**
> NERC Reliability Standards are based on certain reliability principles that define the foundation of reliability for North American bulk power systems. Each reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of reliability of the North American bulk power systems. Each reliability standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.
>
> Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
>
> Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

Principle 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

Principle 7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks. (footnote omitted).

C6. Is there any negative impact on the defense in depth protection of the BES?

The application of this criterion considers whether the requirement proposed for retirement is part of a defense in depth protection strategy. In order words, the assessment is to verify whether other requirements rely on the requirement proposed for retirement to protect the BES.

C7. Does the retirement promote results or performance based Reliability Standards?

The application of this criterion considers whether the requirement, if retired, will promote the initiative to implement results- and/or performance-based Reliability Standards.

IV. The Initial Phase Reliability Standards Requirements Proposed for Retirement

The following lists the requirements proposed for retirement with details of the assessment resulting from the applicability of the criteria above.

BAL-005-0.2b R2 – Automatic Generation Control

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

Background/Commission Directives

BAL-005-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[6] Also, the Commission accepted an errata filing to BAL-005-0.1b, which replaced Appendix 1 with a corrected version of a Commission-approved interpretation, and made an internal reference correction in the interpretation, thus resulting in BAL-005-0.2b.[7]

In Order No. 693 at paragraph 387, the Commission stated that:

> The goal of this Reliability Standard is to maintain Interconnection frequency by requiring that all generation, transmission, and customer load be within the metered boundaries of a balancing authority area, and establishing the functional requirements for the balancing authority's regulation service, including its calculation of ACE.

At paragraph 396, the Commission stated:

> On this issue, the Commission directs the ERO to modify BAL-005-0 through the Reliability Standards development process to develop a process to calculate the minimum regulating reserve for a balancing authority, taking into account expected load and generation variation and transactions being ramped into or out of the balancing authority.

This Commission directive is unaffected by the proposed retirement of BAL-005-0.2b R2.

[6] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[7] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Errata Changes to Seven Reliability Standards, Docket No. RD12-4-000 (September 13, 2012).

Additionally, when adjusting the VRF for the previous version, BAL-005-0.1b R2, from Lower to High, the Commission stated that:[8]

> While theoretically, CPS can be met without the use of AGC, for example, when the AGC system is malfunctioning, the Commission believes, in practice, that AGC is the most dependable and effective means for multiple balancing authorities in an Interconnection to collectively meet CPS requirements in tandem while minimizing assistance from each other in this regard. Human reaction is neither fast enough nor dependable enough in this repetitive task to provide the immediate and continuous support to correct for Interconnection frequency drift. Further, the failure to use AGC presents a higher risk that immediate load shedding will need to be implemented after the sudden loss of generation or an unforeseen significant load increase and, thus, the failure to use AGC subjects the Bulk-Power System to a higher risk of instability.

However, the fact that the VRF for BAL-005-0.2b R2 is High is not indicative of its actual impact on the BES as explained in further detail below. Also, no Commission directive is impacted by BAL-005-0.2b R2.

Technical Justification

The stated reliability purpose of BAL-005-0.2b is to establish requirements for Balancing Authority Automatic Generation Control ("AGC") necessary to calculate Area Control Error ("ACE") and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved. The reliability purpose and objectives of BAL-005-0.2b are unaffected by the proposed retirement of R2.

A Balancing Authority must use AGC to control its Regulating Reserves to meet the Control Performance Standards ("CPS") as set forth in BAL-001-0.1a R1 and R2. Although for a short period of time (as the Commission stated during an AGC malfunction) a Balancing Authority may be able to meet its CPS obligations without AGC, it cannot do so for any extended period of time, and, therefore, Balancing Authorities must use AGC to control its Regulating Reserves to satisfy its obligations under BAL-001-0.1a R1 and R2. Given this fact, it is redundant to also have BAL-005-0.2b R2 set forth the following statement: "Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard." (Criterion B7). It is the duplicative nature of having two requirements requiring the same activity that does little, if anything, to benefit or protect reliable operation of the BES. (Criterion A). In other words, without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a R1 and R2.

[8] *North American Electric Reliability Corporation*, 121 FERC ¶ 61,179 at P 50 (2007).

Also, the retirement of BAL-005-0.2b R2 would increase the efficiency of the ERO compliance program because NERC and the Regional Entities would be able to focus their time and resources on monitoring compliance on BAL-001-0.1a R1 and R2, which are results-based requirements, versus monitoring compliance with both BAL-001-0.1a R1 and R2 as well as the static statement in BAL-005-0.2b R2. Therefore, retiring BAL-005-0.2b R2 will provide for increased efficiencies in the ERO compliance program.

Criterion A

Without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a R1 and R2. Having two requirements requiring a Balancing Authority to conduct the same activity or task does little, if anything, to benefit or protect the reliable operation of the BES because it is duplicative.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. BAL-005-0.2b R2 has not been part of a FFT filing.

2. BAL-005-0.2b R2 is currently scheduled to be included in Standards Development Project 2010-14.2, which is Phase II of Balancing Authority Reliability-based Controls: Time Error, AGC, and Inadvertent. Given that Project 2010-14.2 is currently not an active Standards Development Project, it remains appropriate to retire BAL-005-0.2b R2 via the P81 Project.

3. The VRF for BAL-005-0.2b R2 is High. Given the redundant nature of BAL-005-0.2b R2, the High VRF is not dispositive of whether or not it should be retired since BAL-001-0.1a R1 and R2 accomplishes the important reliability requirement of Balancing Authorities maintaining Regulating Reserves that can be controlled by AGC to satisfy CPS.

4. BAL-005-0.2b R2 is not part of the 2013 AML.

5. The redundant nature of BAL-005-0.2b R2 with BAL-001-0.1a R1 and R2 also indicates that the retirement of BAL-005-0.2b R2 does not pose a negative impact to NERC's published and posted reliability principles. The two reliability principles applicable to BAL-005-0.2b R2 are the following:

    Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement of BAL-005-0.2b R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. As discussed above, given that BAL-001-0.1a R1 and R2 already require that AGC be used to control Regulating Reserves, there is no risk or gap to reliability resulting from the retirement of BAL-005-0.2b R2.

7. Retirement of BAL-005-0.2b R2 promotes a results-based approach, because it is retiring a static requirement while BAL-001.1a R1 and R2, which are more dynamic and results-based requirements, will remain in effect.

Accordingly, for the above reasons, it is appropriate to retire BAL-005-0.2b R2.

CIP-003-3, -4 R1.2 – Cyber Security – Security Management Controls

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[9] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[10] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[11] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[12]

In Order No. 706 at paragraph 342 the Commission stated that:

[9] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).
[10] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[11] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[12] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

> Reliability Standard CIP-003-1 seeks to ensure that each responsible entity has minimum security management controls in place to protect the critical cyber assets identified pursuant to CIP-002-1. To achieve this goal, a responsible entity must develop a cyber security policy that represents management's commitment and ability to secure its critical cyber assets. It also must designate a senior manager to direct the cyber security program and to approve any exception to the policy.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R1.2 does not impact a Commission directive.

Technical Justification

The importance of the cyber security policy as representing management's commitment and ability to secure critical cyber assets is overshadowed by the rigorous and specific training, procedural and process related requirements of the CIP Standards. These trainings, procedures and processes render having the cyber security policy readily available an unnecessary requirement. In other words, whether CIP personnel are completing a typical CIP requirement cyber security task or responding to an immediate situation, they will act via their specific training, processes and procedures and not the overarching cyber security policy. Stated another way, CIP personnel will act via their specific training, processes and procedures which reflect the overarching cyber security policy. Consequently, the cyber security policy's generalized guidance on compliance with the CIP requirements is not a document that adds value to personnel protecting the BES from a cyber attack on a day-to-day basis.

Furthermore, to implement CIP-003-3, -4 R1.2 entities have undertaken a variety of administrative solutions including kiosks dedicated to computers with the cyber security policy, posting the policy on the company intranet, having copies available in work stations, at common area desks in generating stations and substations, etc. Therefore, although the cyber security policy is readily available for all personnel who have access to, or are responsible for, Critical Cyber Assets, these personnel are specifically and appropriately focused on implementing the procedures and processes required by CIP Reliability Standards such as CIP-007-3 R1, which states as follows:

> Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

Generally the cyber security policy will cite CIP-007-3 R1 as a requirement, and may refer to procedures related to CIP-007-3 R1, but will not have, nor is it required to have, the detail necessary to implement CIP-007-3 R1. In some larger companies, it is also common to have specific procedures on how to accomplish requirements such as CIP-007-3 R1 in a control center versus a generating plant or substation, and it may be different CIP personnel implementing these procedures in locations many hundreds of miles, states or Interconnections away from each other. The value of a more general cyber security policy to these individuals is minimal, at best, and, therefore, does not support reliability. Also, making it readily available at all office locations is an unnecessarily burdensome administrative task.

Moreover, to place every procedure and process to comply with CIP in the cyber security policy is also not practical or effective, because such a large policy will only distract from CIP personnel being able to specifically focus on the task before them. As already stated, there are likely some differences between implementing a requirement like CIP-007-1 R1 in a control center that may be located in one state and for generators located several states and hundreds of miles away. Thus, making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES (Criteria A and B1).

In this context, also consider the inefficiencies CIP-003-3, -4 R1.2 may be causing the ERO compliance program. In companies with hundreds of personnel who have access to, or are responsible for, Critical Cyber Assets in multiple states and Interconnections, the ERO may expend a significant amount of time and resources to monitor compliance with CIP-003-3, -4 R1.2 via a review of kiosks, intranet sites, office cubicles, desks, etc in multiple locations. Accordingly, considerable efficiency gains will be obtained for the ERO's compliance program if CIP-003-3, -4 R1.2 is retired.

Criterion A
Making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. CIP-003-3, -4 R1.2 has been part of a FFT filing.[13]

2. As is the case with all the CIP requirements (other than CIP-001-2a R4) proposed for retirement in this technical paper, CIP-003-3, -4 R1.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security) ("CIP V5"). The P81 SDT has coordinated its efforts with the chair of Project 2008-06. There is no conflict between CIP requirements proposed in this technical white paper for

[13] NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

retirement and the direction of Project 2008-06. The CIP V5 requirements are not Board of Trustee or Commission approved, and, even if they were, the effective date of CIP V5 is unknown and likely at least a year, maybe more, into the future. Thus, unlike the other requirements presented here for informational purposes, it is appropriate to maintain all the CIP requirements discussed in this technical paper within the scope of the P81 Project to secure the efficiency gains resulting to the ERO compliance program from their retirement.

3. CIP-003-3, -4 R1.2 has a Lower VRF. As explained above, CIP-003-3, -4 R1.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-003-3,-4 R1.2 is in the second tier of the AML. As explained above, CIP-003-3, -4 R1.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given its administrative nature, CIP-003-3, -4 R1.2 does not negatively impact NERC's published and posted reliability principles. The two reliability principles that appear applicable to CIP-003-3, -4 R1.2 are the following:

   Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

   Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks.

   As stated above, other CIP requirements are replete with the requirements that CIP personnel implement to protect the BES from cyber attacks.

6. Retiring CIP-003-3, -4 R1.2 does not negatively impact defense in depth because no other requirement depends on the cyber security policy being readily available. Therefore, the removal of CIP-003,-3,-4 R1.2 cannot have a negative impact on defense in depth.

7. Retirement of CIP-003-3, -4 R1.2 promotes a results-based approach because the requirement is mechanistic and administrative, and does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R1.2.

CIP-003-3, -4 R3, R3.1, R3.2, R3.3 – Cyber Security – Security Management Controls

R3. Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[14] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[15] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[16] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[17]

In Order No. 706 at paragraphs 373 and 376 the Commission stated that:

> Requirement R3 provides that a responsible entity must document exceptions to its policy with documentation and senior management approval. The Commission is concerned that, if exceptions mount, there would come a point where the exceptions rather than the rule prevail. In such a situation, it is questionable whether the responsible entity is

[14] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).
[15] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[16] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[17] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

> actually implementing a security policy. We therefore believe that the Regional Entities should perform an oversight role in providing accountability of a responsible entity that excepts itself from compliance with the provisions of its cyber security policy. Further, we believe that such oversight would impose a limited additional burden on a responsible entity because Requirement R3 currently requires documentation of exceptions.
>
> Further, the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 do not impact a Commission directive.

Technical Justification

CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 (CIP exception requirements) have proven not to be useful and have been subject to misinterpretation. For instance, although the CIP exception requirements have not been available for use to exempt an entity from compliance with any requirement of any Reliability Standard, based on questions received by NERC CIP Staff, entities may be interpreting the CIP exception requirements to allow for such an exemption. The CIP exception requirements only apply to exceptions to internal corporate policy, and only in cases where the policy exceeds a Reliability Standard requirement or addresses an issue that is not covered in a Reliability Standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of eight characters in length, and be changed every 30 days, which is over and above what is required in CIP-007-3 R5.3, the CIP exception requirements could be invoked for internal governance purposes to lessen the corporate requirement back to the password requirements in CIP-007-3 R5.3, but under no circumstances do the CIP exception requirements authorize the implementation of security measures less than what is required in CIP-007-3 R5.3.

The retirement of the CIP exception requirements would not impact an entity's ability to maintain such an exception process within their corporate policy governance procedures, if it so desired. Consequently, the CIP exception requirements were always an internal administrative and documentation requirement that is outside the scope of the other CIP requirements (Criteria B1 and B3). In this context, the CIP exception requirements do not support the level of reliability set forth in the Reliability Standards, and are unnecessarily burdensome because they have resulted in entities implementing practices

due to a misinterpretation of the requirement that has caused them to allocate time and resources to tasks that are misaligned with the requirements themselves. Unfortunately, this misunderstanding has also impacted the efficiency of the ERO compliance program because of the amount of time and resources needed to clear up the misunderstanding and coach entities on the meaning of the CIP exception requirements. These inefficiencies would be eliminated with the retirement of the CIP exception requirements. Accordingly, as explained, the CIP exception requirements are an administrative tool for internal corporate governance procedures, and, therefore, are not requirements that are necessary or directly protect the BES from a cyber attack, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A).

Criterion A
The CIP exception requirements are a tool for internal corporate governance procedures and is not a requirement directly protecting the BES from a cyber attack, and, therefore, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C

1. The CIP exception requirements have been part of a FFT filing.[18]

2. The CIP exception requirements are part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between the CIP exception requirements proposed in this technical white paper for retirement and the direction of Project 2008-06.

3. The CIP exception requirements each have a Lower VRF. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. The CIP exception requirements are on the third tier of the AML. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the administrative and unnecessary nature of the CIP exception requirements in relation to protecting the BES from cyber attacks, retirement does not pose any negative impact to NERC's published and posted reliability

[18] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-6-000 (December 30, 2011).

principles, of which only Principle 8 appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. Retiring the CIP exception requirements does not negatively impact any defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of the CIP exception requirements promotes a results-based approach because the CIP exception requirements are approaches that entities may voluntarily take to handle internal corporate governance procedures, and, therefore, do not provide the foundation for performing a required reliability task.

Accordingly, for the above reasons, it is appropriate to retire the following CIP exception requirements: CIP-003-3, -4 R3, R3.1, R3.2, and R3.3.

CIP-003-3, -4 R4.2 - Cyber Security – Security Management Controls

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Background/Commission Directives
CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[19] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[20] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[21] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[22] In Order No. 706, the Commission did not specifically address CIP-003-3, -4 R4.2.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R4.2 does not impact a Commission directive.

Technical Justification
The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an unnecessarily

[19] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[20] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[21] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[22] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, (2012).

administrative and a documentation task that is redundant with CIP-003-3, -4 R4 (Criteria A, B1, B3 and B7). Specifically, CIP-003-3, -4 R4[23] already requires the classification of information associated with Critical Cyber Assets. The only difference between R4 and R4.2 is that the subjective term "based on the sensitivity" has been added, thus, making it essentially redundant. Further, CIP-003-3, -4 R4 requires the entity to develop classifications based on a subjective understanding of sensitivity (*i.e.*, no clear connection to serving reliability), the requirement does not support reliability. In this context, classifying based on sensitivity becomes an administrative task that becomes necessarily burdensome, because of all the possible ramifications "based on sensitivity" can produce, and, therefore, require SMEs to decide on and reduce to writing in a documented program. This is time and effort that could be better spent on other CIP activities that provide value to cyber security and actively protect the BES. For similar reasons, retiring CIP-003-3, -4 R4.2 and the term "based on sensitivity" would increase the efficiencies of the ERO compliance program on several levels. The ERO would not spend time and resources on reviewing whether an entity's documentation contained classifications "based on sensitivity," and, instead would be able to focus its time and resources monitoring compliance with the entity's program to identify, classify, and protect information associated with Critical Cyber Assets (R4), without any distraction on monitoring the subjective implementation of classifications based on sensitivity (R4.2).

Criterion A
The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an administrative and a documentation task that is redundant with CIP-003-3, -4 R4.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)
- Criterion B7 (Redundant)

Criteria C

1. CIP-003-3, -4 R4.2 has been part of a FFT filing.[24]

2. CIP-003-3, -4 R4.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-003-3, -4 R4.2 and the direction of Project 2008-06.

[23] "**R4**. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets."
[24] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

3. CIP-003-3, -4 R4.2 has a Lower VRF. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-003-3, -4 R4.2 is on the third tier of the AML. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the unnecessary and redundant nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8 which appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. Retirement of CIP-003-3, -4 R4.2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of CIP-003-3, -4 R4.2 promotes a results-based approach because retiring CIP-003-3, -4 R4.2 moves away from prescriptive, checklist of documentation approach to Reliability Standard requirements.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R4.2.

CIP-005-3a, -4a R2.6 – Cyber Security – Electronic Security Perimeter(s)

R2.6. Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

Background/Commission Directives

CIP-005-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[25] CIP-005-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RD09-7-000 and RM06-22-000 and was approved on September 30, 2009.[26] CIP-005-2a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by

[25] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

[26] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).

unpublished letter order on February 2, 2011.[27] CIP-005-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[28] CIP-005-3a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by an unpublished letter order on February 2, 2011.[29] CIP-005-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No. 761.[30] CIP-005-4a was filed for Commission approval as errata to the CIP Version 4 Petition on April 12, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No 761, the Final Rule on the CIP Version 4 standards.[31]

In Order 706 at paragraph 505 the Commission noted that:

> Requirement R2 of CIP-005-1 requires a responsible entity to implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-005-3, -4 R2.6 does not impact a Commission directive.

Technical Justification

The implementation of an appropriate use banner ("banner") on a user's screen for all interactive access attempts into the Electronic Security Perimeter ("ESP") is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES. Specifically, the banner does not support reliability because people who intend to inappropriately use sites will simply ignore the banner. (Criterion A). The banner is also an administrative task since it simply requires a message be displayed on an access screen. Furthermore, the implementation and administration of a non-beneficial tool, such as the banner, therefore creates a needlessly burdensome task. As mentioned, above, the ineffectiveness of the banner also indicates that it does not support reliability. (Criteria B1 and B3). In addition, banners of this type are generally considered to be a form of legal protection or mitigation of liability, rather than security protection. Furthermore, the banner does not ensure a proper or secure access point configuration

[27] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).
[28] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[29] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).
[30] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).
[31] *Id.*

which is generally the purpose of CIP-005-3a, -4a. Further, this requirement has also been the subject of numerous TFEs for devices that cannot support such a banner, and hence has diverted resources from more productive efforts. Thus, the ERO's compliance program would become more efficient if CIP-005-3a, -4a R2.6 was retired, because ERO time and resources could be reallocated to monitor compliance with the remainder of CIP-005-3a, -4a, which provides for more effective controls of electronic access at all electronic access points into the ESP.

Criterion A

The implementation of an appropriate use banner on a user's screen for all interactive access attempts into the ESP is an activity or task that does little, if anything, to benefit or protect reliable operation of the BES, because it is administrative and a static electronic message that is not an effective deterrent or control against unauthorized access.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C

1. CIP-005-3a, -4a R2.6 has been part of a FFT filing.[32]

2. CIP-005-3a, -4a R2.6 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-005-3a, -4a R2.6 and the direction of Project 2008-06.

3. The VRF for CIP-005-3a, -4a R2.6 is Lower. As explained above, CIP-005-3a, -4a R2.6 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-005-3a, -4a R2.6 is on the first tier of the AML; however, given its clear ineffective nature the placement on the first tier is not dispositive of whether it should be retired.

5. Reliability principle No. 8 – "Bulk power systems shall be protected from malicious physical or cyber attacks" – is not implicated or negatively impacted by the retirement of CIP-005-3a, -4a R2.6, because it is not an effective deterrent or control to unauthorized access into an ESP.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk

[32] NERC FFT Informational Filing, Docket No. RC12-13-000 (June 29, 2012); NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012).

to reliability. Furthermore, the remainder of CIP-005-3a, -4a provides for actual controls of electronic access at all electronic access points which addresses the reliability risk associated with unauthorized access into an ESP.

7. Its retirement also promotes a results-based approach because CIP-005-3a, -4a R2.6 is an ineffective administrative task, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-005-3a, -4a R2.6.

CIP-007-3, -4 R7.3 – Cyber Security – Systems Security Management

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Background/Commission Directives

CIP-007-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[33] CIP-007-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[34] CIP-007-2a was filed for Commission approval on November 17, 2009 in Docket No. RD10-3-000 and was approved on March 18, 2010.[35] CIP-007-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[36] CIP-007-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[37]

In Order No. 706 at paragraph 631 the Commission stated that:

> Requirement R7 of CIP-007-1 requires the responsible entity to establish formal methods, processes and procedures for disposal or redeployment of cyber assets. In the CIP NOPR, the Commission addressed the concern that solely to "erase the data," as stated several times in Requirement R7, may not be adequate because technology exists that allows retrieval of "erased" data from storage devices, and that effective protection requires discarded or redeployed assets to undergo high quality degaussing. We noted that erasure is as much a method as it is a goal, and that the

[33] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[34] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[35] Order Approving Reliability Standard Interpretation, 130 FERC ¶ 61,184 (2010).
[36] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[37] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

> requirement ultimately needs to assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. Degaussing is not the sole means for achieving this goal. The Commission therefore proposed to direct the ERO to modify Requirement R7 to clarify this point. (Footnote omitted)

This Commission directive is unaffected by the retirement of CIP-007-3,-4 R7.3 as explained below.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. [38] CIP-007-3, -4 R7.3 requires the maintaining of records for the purpose of demonstrating compliance with disposing of or redeploying of Cyber Assets in accordance with documented procedures. NERC and the Regions Entities, however, under Section 400 already have the ability to require the production of records to demonstrate compliance, thus it is unnecessary to also state the same in CIP-007-3, -4 R7.3. The maintaining of records is an administrative task, not a task directly related to the protection of the BES from a cyber attack. The maintaining of records is not a task that by itself, or in conjunction with other requirements, supports reliability. Also, the maintaining of the records becomes unnecessarily burdensome in that it requires all records be maintained, which may or may not be necessary to demonstrate compliance via the production of information under Section 400. (Criteria B1 and B2). As mentioned, CIP-007-3, -4 R7.3 does not promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A).

In contrast, the remaining substantive requirements in R7 read as follows:

> R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

[38] Section 401 of NERC's Rules of Procedure provide for collection of data and information necessary to monitor compliance outside the context of Reliability Standards:

> **Data Access** — All Bulk Power System owners, operators, and users shall provide to NERC and the applicable Regional Entity such information as is necessary to monitor compliance with the Reliability Standards. NERC and the applicable Regional Entity will define the data retention and reporting requirements in the Reliability Standards *and compliance reporting procedures.* (emphasis added).

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

An entity's following of these requirements may help to protect BES reliability, but the retention of evidence associated with these requirements does not. Hypothetically, an entity could perform R7, R7.1 and R7.2 flawlessly and protect the BES, but not have any record of it. While this situation may impact a demonstration of compliance, the lack of records does not necessarily directly impact the reliability of the BES or protect it from a cyber attack.

Also, there are some inherent inefficiencies resulting from a small number of Reliability Standard requirements explicitly mandating the collection of data, evidence and records, while most data and information is collected for ERO compliance monitoring purposes without specific data collection language in the Reliability Standards. In this regard, for the ERO, Regional Entities and the entities, Reliability Standards are arguably more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A

CIP-007-3, -4 R7.3 does not promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. CIP-007-3, -4 R7.3 has not been part of a FFT filing.

2. CIP-007-3, -4 R7.3 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-007-3, -4 R7.3 and the direction of Project 2008-06.

3. The VRF for CIP-007-3, -4 R7.3 is Lower. As explained above, CIP-007-3, -4 R7.3 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-007-3, -4 R7.3 is on the first tier of the AML; however, given that it is simply requiring the retention of records the fact that is on the first tier is not dispositive of whether it should be retired.

5. Given the administrative, data collection nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. The retirement does not negatively impact defense in depth because data retention in-and-of-itself is not an activity that other requirements depend on to help cover a reliability gap or risk to reliability.

7. Its retirement promotes a results-based approach because the data collection/retention does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-007-3, -4 R7.3.

EOP-005-2 R3.1– System Restoration from Blackstart Resources

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

Background/Commission Directives

EOP-005-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[39] EOP-005-2 was submitted for Commission approval on December 31, 2009 in Docket No. RM10-16-000 and was approved on March 17, 2011 in Order No. 749.[40] Although the Commission did not address EOP-005-2 R3 directly in Order No. 749, it stated at paragraph 17 the following:

[39] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 (2007).

[40] *System Restoration Reliability Standards*, 134 FERC ¶ 61,215, (March 17, 2011) ("Order No. 749"), *order on clarification*, 136 FERC ¶ 61,030 ("Order No. 749-A") (2011).

> EOP-005-2 and EOP-006-2 clarify the responsibilities of the reliability coordinator and transmission operator in the restoration process and restoration planning and address the Commission's directives in Order No. 693 related to the EOP Standards. By enhancing the rigor of the restoration planning process, the Reliability Standards represent an improvement from the current Standards and will improve the reliability of the Bulk-Power System. The Commission is not directing any modifications to the three new Reliability Standards. Nevertheless, as discussed below, commenters raised several issues for consideration, at the time these standards are next revisited, which we believe could improve these new Reliability Standards

There are no outstanding Commission directives that are affected by the proposed retirement of EOP-005-2 R3.1.

Technical Justification

The reliability purpose of EOP-005-2 is to ensure that plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure that reliability is maintained during restoration and priority is placed on restoring the Interconnection. This reliability purpose is unaffected by the proposed retirement of R3.1.

A review of EOP-005-2 R3.1 indicates that this requirement is redundant with EOP-005-2 R3 and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1, B5 and B7). The primary reason EOP-005-2 R3.1 is unnecessary is that EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes. EOP-005-2 R3 reads:

> Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule.

Consequently, since R3 requires the Transmission Operator to submit its restoration plan to the Reliability Coordinator whether or not there has been a change, R3.1 only adds a separate, duplicative administrative burden for the entity to also confirm that there were no changes based upon another pre-determined schedule. While R3.1 may have attempted to capture the likelihood that unless there have been significant changes to the entity's BES, there would be no change to the restoration plan, this is an insufficient reason to impose a needlessly burdensome, duplicative administrative requirement relative to the language in R3. EOP-005-2 R3.1 is also clearly needlessly burdensome if one considers that the time and resources of Transmission Operators is better spent reliably operating the BES, rather than submitting paperwork to a Reliability Coordinator on possibly two different pre-determined schedules – one for changes and one for no

changes. For these reasons, there is no reliability gap resulting from the retirement of EOP-005-2 R3.1 because Transmission Operators already have an obligation to review and provide its restoration plan annually on a mutually agreed predetermined schedule to its Reliability Coordinator. It could also be argued that a reason for both R3 and R3.1 is for the Reliability Coordinator to organize the Transmission Operator submittals into changes versus no changes. However, with the requirement to annually review restoration plans comes the need to demonstrate and track annual reviews via the revision history index, for example, which quickly shows the Reliability Coordinator when changes have and have not occurred.

The retirement of EOP-005-2 R3.1 would also increase the efficiencies of the ERO compliance program because the ERO would be able to focus its time and resources on R3 which already captures R3.1 and not be concerned with tracking the submission of restoration plans on multiple pre-determined schedules, some with changes and some without changes. Instead, the focus of the ERO compliance program would be on whether the Transmission Operators annually submitted its restoration plan to its Reliability Coordinator on one pre-determined schedule. Thus, the retirement of EOP-005-2 R3.1 appears to benefit the ERO compliance program.

Criterion A
EOP-005-2 R3.1 is redundant and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B5 (Periodic Updates)
- Criterion B7 (Redundant)

Criteria C

1. EOP-005-2 R3.1 has not been part of a FFT filing.

2. EOP-005-2 R3.1 is not part of an on-going Standards Development Project.

3. EOP-005-2 R3.1 does not yet have a FERC-approved VRF.

4. EOP-005-2 R3.1 is on the second tier of the AML; however, the duplicative nature of R3 and R3.1 discounts any indication that R3.1 being in the second tier is a reason not to proceed with its retirement.

5. Since EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes, retirement of EOP-005-2 R3.1 does not pose any negative impact to the following of NERC's published and posted reliability principles that appear to apply:

Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

6. Retirement of EOP-005-2 R3.1 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of EOP-005-2 R3.1 promotes a results-based approach because the requirement is administrative and unnecessary, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire EOP-005-2 R3.1.

FAC-002-1 R2 – Coordination of Plans for New Facilities

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

Background/Commission Directives

FAC-002-0 was submitted to the Commission for approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[41] FAC-002-1 was submitted for Commission approval on September 9, 2010 in Docket No. RD10-15-000 and was approved on January 10, 2011.[42] When approving FAC-002-0 in Order No.

[41] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[42] NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2 RD10-15-000 (January 10, 2011).

693 at paragraphs 692 and 693, and FAC-002-1 in a subsequent order,[43] the Commission did not directly address R2.

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-002-1 R2.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, without the existence of FAC-002-1 R2, a Regional Entity or NERC has the ability to request and receive "documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems)." This generally would occur during a spot check or compliance audit where entities have the obligation to provide documentation sufficient to demonstrate compliance. In this regard, entities already have the obligation to produce the same information required in R2 to demonstrate compliance to R1 and its sub-requirements, thus making R2 unnecessary. To have a Reliability Standard requirement that is setting forth a data retention requirement and a requirement for the entity to deliver, upon request, that data to NERC or a Regional Entity is unnecessary and also repetitive with the NERC Rules of Procedure. Accordingly, retiring FAC-002-1 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. Thus, FAC-002-1 R2 is not necessary to support reliability. Consequently, a review of R2 indicates that it is an administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). The compilation of three years of data is a burdensome task, particularly when one considers the resources and time spent on stockpiling this information is better spent coordinating the studies, executing an interconnection agreement and ensuring that interconnections are safely and reliably energized, maintained and operated. Also, there are some inherent inefficiencies that result from a small number of requirements, such as CIP-007-3, -4 R7.3 and FAC-002-1 R2 being data, evidence and record retention requirements, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A

A review of FAC-002-1 R2 indicates that it is an administrative and data collection requirement that does little, if anything, to benefit or protect reliable operation of the BES.

[43] *North American Electric Reliability Corporation*, 134 FERC ¶ 61,015 (2011).

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. FAC-002-1 R2 has not been part of a FFT filing.

2. FAC-002-1 R2 is subject to a future Project 2010-02 Connecting New Facilities to the Grid (a review of FAC-001 and FAC-002) that is scheduled to begin in the second quarter of 2015. It seems appropriate to retire FAC-002-1 R2 at this time as it may also make the review of FAC-001 and FAC-002 more effective and efficient.

3. FAC-002-1 R2 has a Lower VRF.

4. FAC-002-1 R2 is in the third tier of the AML.

5. The retirement of FAC-002-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since there are no directly applicable reliability principles.

6. The retirement does not negatively impact defense in depth because the compilation of studies for three years has no operational or planning relationship with any other requirement.

7. The retirement of FAC-002-1 R2 promotes a results-based approach since the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-002-1 R2.

FAC-008-1 R2; FAC-008-1 R3;[44] - Facility Ratings Methodology

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the

[44] Unlike the other requirements presented for informational purposes only, FAC-008-1 R2 and FAC-008-1 R3 have been maintained within the scope of P81 given that they are essentially identical to FAC-008-3 R4 and FAC-008-3 R5. Inclusion would also appear to be consistent with increasing ERO compliance program efficiencies. FAC-008-1 R2 and FAC-008-1 R3 became inactive on December 31, 2012, due to FAC-008-3 becoming enforceable on January 1, 2013.

associated Facilities are located, within 15 business days of receipt of a request.

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

Background/Commission Directives

FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[45]

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-1 R2 and R3.

Technical Justification

FAC-008-1 R2 and R3 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-1 R2 and R3 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-1 regarding their facility rating methodologies whether or not the exchange envisioned by FAC-008-1 R2 and R3 occurs. Furthermore, neither FAC-008-1 R2 and R3 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-1 R2 and R3 are designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its generator step up ("GSU") transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at

[45] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, operating conditions, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of System Operating Limits ("SOLs"), Interconnection Reliability Operating Limits ("IROLs"), calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments).[46] Accordingly, the requirements in FAC-008-1 R2 and FAC-008-1 R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange of comments and compliance with the substantive requirements of FAC-008-1. Instead of spending time and resources on FAC-008-1 R2 and R3, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-1.

Criterion A

The requirements in FAC-008-1 R2 and R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-008-1 R2 and R3 have not been part of a FFT filing.

[46] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-02 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element.

2. FAC-008-1 R2 and R3 are not subject to an on-going Standards Development Project.

3. FAC-008-1 R2 and R3 have a Lower VRF.

4. FAC-008-1 R2 and R3 are in the third tier of the AML.

5. The retirement of FAC-008-1 R2 and R3 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-008-1 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-1 R2 and R3, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These requirements may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-1 R2 and R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-1 R2 and R3.

FAC-008-3 R4; FAC-008-3 R5 – Facility Ratings

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have

responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.

Background/Commission Directives

FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[47] "On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No. 693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[48] FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[49]

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-3 R4 and R5.

Technical Justification

FAC-008-3 R4 and R5 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-3 R4 and R5 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-3 regarding their facility rating methodologies whether or not the exchange envisioned by FAC-008-3 R4 and R5 occurs. Further, neither FAC-008-3 R4 nor R5 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-3 R4 and R5 are

[47] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[48] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[49] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).

designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its GSU transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, historical performance, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of SOLs, IROLs, calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments).[50] Accordingly, the requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-008-3. Instead of spending time and resources on FAC-008-3 R4 and R5, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-3. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-3.

Criterion A

The requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

[50] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-2 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element. Also, FAC-008-3 R7 and R8 require the transmission of facility ratings to reliability entities.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-008-3 R4 and R5 have not been part of a FFT filing.

2. FAC-008-3 R4 and R5 are not subject to an on-going Standards Development Project.

3. FAC-008-3 R4 and R5 have a Lower VRF.

4. FAC-008-3 R4 and R5 are in the third tier of the AML.

5. The retirement of FAC-008-3 R4 and R5 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-008-3 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-3 R4 and R5, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-3 R4 and R5 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-3 R4 and R5.

***FAC-010-2.1 R5 – System Operating Limits Methodology for the Planning Horizon*

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives
FAC-010-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[51] FAC-010-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[52] FAC-010-2.1 was filed for Commission approval on November 20, 2009 in Docket No. RD10-9-000 and was approved on April 19, 2010.[53] In Order No. 722,[54] the Commission approved FAC-010-2.1 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

Technical Justification
The reliability purpose of FAC-010-2.1, to ensure that System Operating Limits used in the reliable planning of the BES are determined based on an established methodology, is unaffected by the proposed retirement of R5. FAC-010-2.1 R5 requires that when a Planning Authority receives comments on its SOL methodology, it must respond and indicate whether it has changed its methodology. The retirement of FAC-010-2.1 R5 does not create a reliability gap, because the Planning Authority must comply with the substantive requirements of FAC-010-2.1 whether or not the exchange envisioned by FAC-010-2.1 R5 occurs. FAC-010-2.1 R5 may support an avenue to advance commercial interests.

For example, if a Transmission Operator or Transmission Planner is also a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Planning Authority's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of its development of a facility ratings methodology

[51] *Facilities Design, Connections and Maintenance Reliability Standards*, 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).
[52] *Version Two Facilities Design, Connections and Maintenance Reliability Standards*, 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).
[53] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Transmission Operations Reliability Standards, Docket No. RD10-9-000 (April 19, 2010).
[54] *Version Two Facilities Design, Connections and Maintenance Reliability Standards* 125 FERC ¶ 61,040 (2009).

under FAC-008-1, -3 than the Planning Authority's methodology. FAC-010-2.1 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Planning Authority's SOL methodology. Accordingly, FAC-010-2.1 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-010-2.1. Instead of spending time and resources on FAC-010-2.1, a Planning Authority's time and resources would be better spent complying with the substantive requirements of FAC-010-2.1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Planning Authority's adherence to substantive requirements of FAC-010-2.1.

Criterion A
The requirement in FAC-010-2.1 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-010-2.1 R5 has not been part of a FFT filing.

2. FAC-010-2.1 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011. Thus, it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-010-2.1 R5 has a Lower VRF.

4. FAC-010-2.1 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

It is the adherence to the substantive requirements of FAC-010-2.1 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-010-2.1 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-010-2.1 R5.

***FAC-011-2 R5– System Operating Limits Methodology for the Operations Horizon*

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives

FAC-011-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[55] FAC-011-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[56] In Order No. 722, the Commission approved FAC-011-2 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

[55] *Facilities Design, Connections and Maintenance Reliability Standards,* 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).

[56] *Version Two Facilities Design, Connections and Maintenance Reliability Standards,* 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).

Technical Justification
FAC-011-2 R5 requires that when a Reliability Coordinator receives comments on its SOL methodology that it must respond and indicate whether it has changed its methodology. The retirement of FAC-011-2 R5 does not create a reliability gap, because the Reliability Coordinator must comply with the substantive requirements of FAC-011-2 R5 whether or not the exchange envisioned by FAC-011-2 R5 occurs. FAC-011-2 R5 may support an avenue to advance commercial interests.

For example, similar to FAC-010-2.1 R5, if a Transmission Operator or Transmission Planner also is a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Reliability Coordinator's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of the development of its facility ratings methodology under FAC-008-1, -3 than the Reliability Coordinator's methodology. FAC-011-2 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Reliability Coordinator's SOL methodology. Accordingly, FAC-011-2 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-011-2. Instead of spending time and resources on FAC-011-2 R5 a Reliability Coordinator's time and resources would be better spent complying with the substantive requirements of FAC-011-2 R5. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-011-2 R5.

Criterion A
The requirement in FAC-011-2 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-011-2 R5 has not been part of a FFT filing.

2. FAC-011-2 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011which is not currently scheduled and thus it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-011-2 R5 has a Lower VRF.

4. FAC-011-2 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-011-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-011-2 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-011-2 R5.

FAC-013-2 R3 – Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made

> to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.

Background/Commission Directives
FAC-013-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[57] FAC-013-2 was submitted for Commission approval on January 28, 2011 in Docket No. RD11-3-000 and was approved on November 17, 2011.[58]

In Order No. 729, the Commission denied NERC's request to withdraw FAC-012-1 and retire FAC-013-1, and directed as follows at paragraph 291:

> 291. The Commission hereby adopts its NOPR proposal to deny NERC's request to withdraw FAC-012-1 and retire FAC-013-1. Instead, pursuant to section 215(d)(5) of the FPA and section 39.5(f) of our regulations, the Commission directs the ERO to develop modifications to FAC-012-1 and FAC-013-1 to comply with the relevant directives of Order No. 693 and, as otherwise necessary, to make the requirements of those Reliability Standards consistent with those of the MOD Reliability Standards approved herein as well as this Final Rule. These modifications should also remove redundant provisions for the calculation of transfer capability addressed elsewhere in the MOD Reliability Standards. In making these revisions, the ERO should consider the development of a methodology for calculation of inter-regional and intra-regional transfer capabilities. The Commission accepts the ERO's request for additional time to prepare the modifications and so directs the ERO to submit the modifications to FAC-012-1 and FAC-013-1 no later than 60 days before the MOD Reliability Standards become effective.

Although the Commission did not directly address the merits of FAC-013-2 R3 when approving FAC-013-2,[59] similar to FAC-008-3, the developer of the Transfer Capability methodology and data must follow specific technical requirements and provide the data to reliability entities for use in their models. There are no outstanding Commission directives with respect to this R3.

Technical Justification
A review of FAC-013-2 R3 indicates that it is a needlessly burdensome administrative task that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B4). Specifically, FAC-013-2 R1 and its sub-requirements set forth the information that each Planning Authority must include when developing its Transfer Capability methodology. FAC-013-2 R3 sets forth a requirement that if an entity

[57] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[58] *Order Approving Reliability Standard*, 137 FERC ¶ 61,131 (2011).
[59] *Id.* (approval of FAC-013-2).

comments on this methodology, the Planning Authority must respond and indicate whether or not it will make a change to its Transfer Capability methodology. Thus, while R1 sets forth substantive requirements, R3 sets forth more of an administrative task of the Planning Authority responding to comments on its methodology.

The following NERC glossary definition of Transfer Capability states:

> The measure of the ability of interconnected electric systems to move or transfer power *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is *not g*enerally equal to the transfer capability from "Area B" to "Area A."

In the context of a Planning Authority engaging in an exchange with an entity over the Transfer Capability there is a possibility of a scenario that a group of generators[60] try to get the Planning Authority to revise its Transfer Capability methodology to advance commercial interests via changes to the methodology that would increase or decrease transfer capability from Area A to Area B. (Criterion B6). Such issues should be raised in the context of receipt of transmission services, not the Reliability Standards. Moreover, even without the possible commercial motivation of certain entities to get the Planning Authority to revise its Transfer Capability methodology, implementing an exchange between entities and the Planning Authority seems much better suited via regional planning committees, than mandatory Reliability Standards.

In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-013-2. Instead of spending time and resources on FAC-013-2 R3, time and resources would be better spent complying with the substantive requirements of FAC-013-2. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-013-2.

Criterion A

The requirement in FAC-013-2 R3 to respond to comments on the Transfer Capability methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

[60] Generators that receive the Transfer Capability methodology via an association with one of the entities in the R2 sub-requirements.

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-013-2 R3 has not been part of a FFT filing.

2. FAC-013-2 R3 is not subject to an on-going Standards Development Project.

3. FAC-013-2 R3 has a Lower VRF.

4. FAC-013-2 R3 is not on the AML.

5. The retirement of FAC-013-2 R3 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-013-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of FAC-013-2 R3 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-013-2 R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-013-2 R3.

INT-007-1 R1.2 – Interchange Confirmation

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

Background/Commission Directives
INT-007-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[61] The Commission did not directly address INT-007-1 R1.2 when it approved the Reliability Standard in Order No. 693 at paragraph 867.

There are no outstanding Commission directives with respect to R1.2.

Technical Justification
The reliability purpose of INT-007-1 is to ensure that each Arranged Interchange is checked for reliability before it is implemented. The reliability purpose of INT-007-1 is unaffected by the proposed retirement of R1.2.

INT-007-1 R1.2 is a needlessly burdensome administrative task that does not support reliability because it is now outdated. (Criterion B1). At one time the identification number came from the NERC TSIN system, by now it is handled via NAESB Electric Industry Registry.[62] Also, under the E-Tag protocols, no entity may engage in an Interchange transaction without first registering with the E-Tag system and receiving an identification number. Further, the entity desiring the transaction enters this identification number in the E-Tag system to pre-qualify and engage in an Arranged Interchange. Accordingly, the task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A). The ERO compliance program would benefit and be more efficient if it was not monitoring an outdated requirement.

Criterion A
The task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)

Criteria C
1. INT-007-1 R1.2 has not been part of a FFT filing.

2. INT-007-1 R1.2 is part of a pending Standards Development Project – Project 2008-12 Coordinate Interchange Standards, which is estimated to start in the

[61] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[62] *See, North American Energy Standards Board Webregistry Technical Guide v1.4* (Proprietary) (July 2012). The new NAESB system has updated and implemented more automation to the process.

second quarter of 2013. Given this timeline, it is appropriate to move forward with the retirement of INT-007-1 R1.2. Such a retirement may also help to streamline Project 2008-12 once it is active and progressing.

3. INT-007-1 R1.2 has a Lower VRF.

4. INT-007-1 R1.2 is not on the AML.

5. The retirement of INT-007-1 R1.2 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of INT-007-1 that promotes these posted reliability principles, not R1.2.

6. The retirement of INT-007-1 R1.2 does not impact any defense in depth strategies because the task is no longer necessary.

7. The retirement of INT-007-1 R1.2 promotes a results-based approach because the requirement does not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire INT-007-1 R1.2.

IRO-016-1 R2 – Coordination of Real-time Activities Between Reliability Coordinators

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

Background/Commission Directives

IRO-016-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693. The Commission

did not directly address R2 when approving IRO-016-1 in Order No. 693 at paragraphs 1004 and 1005. There are no outstanding Commission directives with respect to R2.

Technical Justification

The reliability purpose of IRO-016-1 is to ensure that each Reliability Coordinator's operations are coordinated such that they will not have an adverse reliability impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations. To implement the purpose, IRO-016-1 R1 and its sub-requirements state:

> **R1.** The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
>
> **R1.1.** If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.
>
> **R1.2.** If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
>
> **R1.2.1.** If time permits, this re-evaluation shall be done before taking corrective actions.
>
> **R1.2.2.** If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

These requirements are specific actions and decision points among Reliability Coordinators that promote the reliable operation of the BES. In contrast, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Therefore, the reliability purpose of IRO-016-1 is unaffected by the proposed retirement of R2.

Furthermore, outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, the retirement of IRO-016-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to demonstrate

compliance with IRO-016-1 R1 and its sub-requirements. Accordingly, retiring IRO-016-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. Thus, IRO-016-1 R2 does not support reliability. Consequently, R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as IRO-016-1 R2 being a data, evidence and record retention requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A
A review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C
1. IRO-016-1 R2 has not been part of a FFT filing

2. IRO-016-1 R2 is not subject to an on-going Standards Development project.

3. IRO-016-1 R2 has a Lower VRF.

4. IRO-016-1 R2 is not on the AML.

5. The retirement of IRO-016-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since none of the principles appear to apply to a data retention requirement.

6. IRO-016-1 R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of IRO-016-1 R2 promotes a results-based approach because the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire IRO-016-1 R2.

NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4 – Nuclear Plant Interface Coordination

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement.

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3. A requirement to review the agreement(s) at least every three years.

R9.1.4. A dispute resolution mechanism.

Background/Commission Directives

NUC-001-1 was submitted for Commission approval on November 19, 2007 in Docket No. RM08-3-000 and was approved on October 16, 2008.[63] NUC-001-2 was submitted for Commission approval on August 14, 2009 in Docket No. RD09-10-000 and was approved on January 21, 2010.[64]

Although in Order No. 716 the merits of R9.1 and its sub-requirements were not directly addressed, the Commission did state the following in the context of the VRFs for all of R9:[65]

> Consistent with the NOPR, the Commission directs the ERO to revise the violation risk factor assignment for Requirement R9 from lower to medium. The Commission disagrees with commenters that a lower violation risk factor is appropriate because Requirement R9 is an administrative requirement to include the specified provisions. While the Commission recognized in the NOPR that many of the requirements of the proposed Reliability Standard are administrative in nature, these same requirements provide for the development of procedures to ensure the safe and reliable operation of the grid, and responses to potential emergency conditions.

There are no outstanding Commission directives with respect to these requirements.

---

[63] *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008) ("Order No. 716"), *order on reh'g*, Order No. 716-A, 126 FERC ¶ 61,122 (2009).

[64] *Order Approving Reliability Standard*, 130 FERC ¶ 61,051 (2010).

[65] NUC-001-1 was approved in Order No. 716, while NUC-001-2 was approved without discussion of R9.1 and its sub-requirements in a subsequent order. *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008); 130 FERC ¶ 61,051 (2010).

Technical Justification

The reliability purpose of NUC-001-2 is to ensure the coordination between Nuclear Plant Generator Operators and Transmission Entities for nuclear plant safe operation and shutdown. The reliability purpose of NUC-001-2 is unaffected by the proposed retirement of requirements 9.1, 9.1.1, 9.1.2, 9.1.3 and 9.1.4. Requirement 9.1 and its sub-requirements specify certain administrative elements that must be included in the agreement (required by R2) between the Nuclear Plant Generator Operator and the applicable Transmission Entities. These are a mix of technical, communication, training and administrative requirements. Of those that may be classified as administrative, R9.1 and its sub-requirements clearly stand out as unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A and B1). R9.1 and its sub-requirements are a check list of certain non-technical boilerplate provisions generally included in modern agreements. These provisions do not directly relate to protecting BES reliability. Further, requiring via a mandatory Reliability Standard the inclusion of boilerplate provisions is unnecessarily burdensome relative to the other significant requirements in NUC-001-2 that pertain to performance based reliability coordination and protocols between Transmission Entities and Nuclear Plant Generator Operators. Therefore, the retirement of NUC-001-2 R9.1 and all its sub-requirements creates no reliability gap and are the type of provisions that would likely be in a modern agreement anyway.

For these same reasons, the ERO compliance program efficiency will increase with the retirement of NUC-001-2 R9.1 and its sub-requirements because compliance monitoring time and resources will not be spent conducting a checklist of whether an agreement includes boilerplate provisions, and instead, the time and resources may be spent reviewing adherence with the technical, substantive coordination and protocol provisions of NUC-001-2.

Criterion A

R9.1 and its sub-requirements are unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. NUC-001-2 R9.1 and its sub-requirements have not been part of a FFT filing.

2. NUC-001-2 R9.1 and its sub-requirements are not part of an on-going Standards Development Project, but NUC-001-2 is part of Project 2012-13, which is a placeholder for a five year review. Given the as yet undetermined start date for Project 2012-13, it is appropriate to move forward with the retirement of NUC-001-2 R9.1 and its sub-requirements.

3. Individual VRFs are not assigned to the sub-requirements of NUC-001-2 R9.

4. NUC-001-2 R9.1 and its sub-requirements are in the third tier of the AML.

5. The retirement of NUC-001-2 R9.1 and its sub-requirements do not pose any negative impact to NERC's published and posted reliability principles, since none of them seem to apply to the inclusion of boilerplate contractual provisions.

6. There is no impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of NUC-001-2 R9.1 and its sub-requirements promote a results-based approach by eliminating administrative check-list requirements.

Accordingly, for the above reasons, it is appropriate to retire NUC-001-2 R9.1 and its sub-requirements.

PRC-010-0 R2 – Assessment of the Design and Effectiveness of UVLS Program;

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

Background/Commission Directives

PRC-010-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[66] Although not specifically addressing PRC-010-0 R2, in Order No. 693 at paragraph 1506 and 1507 the Commission stated that:

> With regard to ISO-NE's disagreement on integration of various system protections "because such integration cannot be technologically accomplished", we note that the evidence collected in the Blackout Report indicates that "the relay protection settings for the transmission lines, generators and underfrequency load shedding in the northeast may not be entirely appropriate and are certainly not coordinated and integrated to reduce the likelihood and consequence of a cascade – nor were they intended to do so." In addition, the Blackout Report stated that one of the common causes of major outages in North America is a lack of coordination on system protection. The Commission agrees with the

[66] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

> protection experts who participated in the investigation, formulated Blackout Recommendation No. 21 and recommended that UVLS programs have an integrated approach.
>
> Regarding FirstEnergy's question of whether universal coordination among UVLS programs that address local system problems makes sense, we believe that PRC-010-0's objective in requiring an integrated and coordinated approach is to address the possible adverse interactions of these protection systems among themselves and to determine whether they could aggravate or accelerate cascading events. We do not believe this Reliability Standard is aimed at universal coordination among UVLS programs that address local system problems. (Footnote omitted).

The retirement of PRC-010-0 R2 does not affect a Commission directive.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its current UVLS program assessment for purposes of monitoring compliance. Thus, the retirement of PRC-010-0 R2 does not affect the ability of NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-010-0 R1 and its sub-requirements. Furthermore, PRC-010-0 R1 requires that the entity document an assessment of the effectiveness of its UVLS program:

> The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program.

Accordingly, retiring PRC-010-0 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. A review of R2 indicates that it is a needlessly burdensome administrative and data collection/retention requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as PRC-010-0 R2 being a data production requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401.

Criterion A

R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. PRC-010-0 R2 has not been part of a FFT filing.

2. PRC-010-0 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-010-0 R2 in the P81 Project.

3. This requirement has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-010-0 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-010-0 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-010-0 R2.

PRC-022-1 R2 – Under-Voltage Load Shedding Program Performance

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

Background/Commission Directives

PRC-022-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[67] In Order No. 693 at paragraph 1565 the Commission approved PRC-022-1 without a discussion of R2. There are no outstanding Commission directives with respect to R2.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its analysis of UVLS program performance for purposes of monitoring compliance. Thus, the retirement of PRC-022-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-022-1 R1 and its sub-requirements. Furthermore, PRC-022-1 R1 already requires that the entity document UVLS performance:

> Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations.

Accordingly, retiring PRC-022-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. In this context, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, similar to the retention of records requirements in CIP-007-3, -4 R7.3, FAC-002-1 R2 and PRC-010-0 R2, the ERO compliance program efficiency will increase since it will no longer need to track a static requirement of whether a UVLS program assessment was submitted within 30 days of a request by NERC or the Regional Entity, and instead, compliance monitoring may focus on the more substantive requirements of PRC-022-1.

Criterion A

R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. PRC-022-1 R2 has not been part of a FFT filing.

[67] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

2. PRC-022-1 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-022-1 R2 in the P81 Project.

3. PRC-022-1 R2 has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-022-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-022-1 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-022-1 R2.

***VAR-001-2 R5 – Voltage and Reactive Control*

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

Background/Commission Directives
VAR-001-1 was submitted for Commission approval on April 4, 2006, in Docket No. RM06-16-000. When approving VAR-001-1, in Order No. 693 at paragraph 1858,[68] the Commission recognized:

> . . . that all transmission customers of public utilities are required to purchase Ancillary Service No. 2 under the OATT or self-supply, but the OATT does not require them to provide information to transmission

[68] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

> operators needed to accurately study reactive power needs. The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities.

On September 9, 2010, NERC submitted VAR-001-2, which included revisions to Requirement R5 to satisfy Commission directives in Order No. 693, including the directive in paragraph 1858. This directive was addressed by adding "Load Serving Entities" to the standard as applicable entities and making them subject to the same requirements as Purchasing Selling Entities. These modifications to VAR-001-2 were accepted by the Commission on January 10, 2011.[69]

Technical Justification

VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* open access transmission tariff ("OATT"). (Criteria A and B7). To elaborate, VAR-001-2 R5 provides for the PSE and LSE (transmission customers) to arrange for or self provide reactive resources the same as required under Schedule 2 of the OATT. Specifically, as a general matter Schedule 2 of the OATT states:

> **Schedule 2 Reactive Supply and Voltage Control from Generation or Other**
>
> In order to maintain transmission voltages on the Transmission Provider's transmission facilities within acceptable limits, generation facilities and non-generation resources capable of providing this service that are under the control of the control area operator) are operated to produce (or absorb) reactive power. Thus, Reactive Supply and Voltage Control from Generation or Other Sources Service must be provided for each transaction on the Transmission Provider's transmission facilities. The amount of Reactive Supply and Voltage Control from Generation or Other Sources Service that must be supplied with respect to the Transmission Customer's transaction will be determined based on the reactive power support necessary to maintain transmission voltages within limits that are generally accepted in the region and consistently adhered to by the Transmission Provider.
>
> Reactive Supply and Voltage Control from Generation or Other Sources Service is to be provided directly by the Transmission Provider (if the Transmission Provider is the Control Area operator) or indirectly by the Transmission Provider making arrangements with the Control Area operator that performs this service for the Transmission Provider's Transmission System. The Transmission Customer must purchase this service from the Transmission Provider or the Control Area operator. A

[69] *North American Electric Reliability Corp.*, 134 FERC ¶ 61,015 (2011).

> Transmission Customer may satisfy all or part of its obligation through self provision or purchases provided that the self-provided or purchased reactive power reduces the Transmission Provider's reactive power requirements and is from generating facilities under the control of the Transmission Provider or Control Area operator. The Transmission Customer's Service Agreement shall specify any such reactive supply arrangements. To the extent the Control Area operator performs this service for the Transmission Provider, charges to the Transmission Customer are to reflect only a pass-through of the costs charged to the Transmission Provider by the Control Area operator. The Transmission Provider's rates for Reactive Supply and Voltage Control from Generation Sources Services shall be set out in Appendix A to this Schedule.

Given the importance of the procurement or self providing of reactive power, even in a market setting a form of Schedule 2 is found in the tariffs of MISO and PJM, for example. Also, other contractual mechanism, such as Interchange agreements, also are used to ensure transmission customers (suc as PSEs and LSEs) provide reactive power, While NERC complied with the Commission's directive to add LSEs to VAR-001-2 R5, a review of this requirement in light of Schedule 2 indicates that the reliability objective of ensuring that PSEs as well as LSEs either acquire or self provide reactive power resources associated with its transmission service requests is accomplished via Schedule 2, and, therefore, there is no need to reiterate it in VAR-001-2 R5. The repetitive nature of VAR-001-2 R5 is also apparent in the context of how a PSE or LSE generally demonstrates compliance – via screenshots from Open Access Same-Time Information System ("OASIS") reservations that show the mandatory acquiring or self providing of reactive power resources per Schedule 2.

The reliability objective of VAR-001-2 is also accomplished in VAR-001-2 R2 (that is not proposed for retirement) which reads:

> Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, [sic] and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

The Transmission Operator's adherence to R2 is a double check for the obligations under Schedule 2 to ensure there are sufficient reactive power resources to protect the voltage levels under normal and Contingency conditions. This double check, however, does not relieve PESs and LESs from their obligations under Schedule 2 of the OATT or Interchange agreements.

In addition, in the Electric Reliability Council of Texas (ERCOT) region, where there is no FERC approved OATT, reactive power is handled via Section 3.15 of the ERCOT

Nodal Protocols that describes how ERCOT establishes a Voltage Profile for the grid, and then in detail explains the responsibilities of the Generators, Distribution Providers and Texas Transmission Service Providers (not to be confused with a NERC TSP), to meet the Voltage Profile and ensure that those entities have sufficient reactive support to do so. There is further Operating Guide detail on the responsibilities for entities to deploy reactive resources approximately, within performance criteria in the Operating Guide Section 3. Thus, as in non-ERCOT regions, ERCOT has protocols that are duplicative of VAR-001-2 R5.

Given the redundant nature of VAR-001-2 R5 it would also assist the ERO compliance program to retire it, so that time and resources can be reallocated to focus on adherence to other Reliability Standard requirements.

Criterion A
VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* OATT.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. VAR-001-2 R5 has not been part of a FFT filing.

2. VAR-001-2 R5 is subject to Standards Development Project 2008-01 Voltage and Reactive Planning Control. Given that Project 2008-01 is not currently active and is only estimated to be completed until the second quarter of 2014 and the purpose of this project does not necessarily include a review of R5, it is appropriate to include VAR-001-2 R5 in the P81 Project. Also, retiring this requirement via P81 Project may facilitate the efficiency of Project 2008-01.

3. This requirement has a High VRF. However, the reliability objective of VAR-001-2 R5 will be accomplished via Schedule 2 of the OATT, ERCOT protocols and R2 of VAR-001-2. Thus, the High VRF is not dispositive, and VAR-001-2 R5 remains appropriate for retirement.

4. VAR-001-2 R5 is in the third tier of the AML.

5. Because VAR-001-2 R5 is redundant with the *pro forma* OATT and ERCOT protocols, (as well as the reliability objective of VAR-001-2 R5 is accomplished via Schedule 2 of the OATT, ERCOT protocols and R2 of VAR-001-2), the retirement of VAR-001-2 R5 does not pose any negative impact to the following NERC published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under

normal and abnormal conditions as defined in the NERC Standards.

Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of VAR-001-2 R5 is neutral regarding whether it promotes a results-based approach because the requirement is results-based, but already covered in the *pro forma* OATT, Schedule 2 and ERCOT protocols.

Accordingly, for the above reasons, it is appropriate to retire VAR-001-2 R5.

V. The Initial Phase Reliability Standards Provided for Informational Purposes

The following requirements are already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the NERC Board of Trustees in November), and, thus, are presented here for informational purposes only. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the NERC Board of Trustees for approval or filed with the Commission or Canadian governmental authorities as part of the P81 Project.

CIP-001-2a R4 Sabotage Reporting

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

Background

CIP-001-1 was filed for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[70] CIP-001-1a was filed for Commission approval on April 21, 2010 in Docket No. RD10-11-000, and was approved by an unpublished letter order on February 2, 2011.[71]

CIP-001-2a was filed for Commission approval as a Regional Variance for the ERCOT Region, containing an interpretation of CIP-001-1, on June 21, 2011 in Docket No. RD11-6-000 and was approved by unpublished letter order on August 2, 2011.[72]

As part of EOP-004-2, on November 5, 2012, stakeholders approved the retirement of CIP-001-2a R4. EOP-004-2 was approved by the NERC Board of Trustees on November 7, 2012. Thus, CIP-001-2a R4 is presented here for informational purposes only.

COM-001-1.1 R6- Telecommunications

Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."

Background

COM-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[73] COM-001-1.1 was submitted for Commission approval on February 6, 2009 in Docket No. RD09-2-000 as errata and was approved by unpublished letter order on May 13, 2009.[74]

As part of COM-001-2, on September 17, 2012, stakeholders approved the retirement of COM-001-1.1 R6 in Project 2006-06 (Reliability Coordination). This project is due to be presented to the NERC Board of Trustees in November. Thus, COM-001-1 R6 is presented here for informational purposes only.

EOP-004-1 R1 – Disturbance Reporting

[70] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[71] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-001-1 —Cyber Security— Sabotage Reporting, Requirement R2, Docket No. RD10-11-000 (February 2, 2011).
[72] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of the Reliability Standard CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity, Docket No. RD11-6-000 (August 2, 2011).
[73] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[74] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Reliability Coordination and Transmission Operations Reliability Standards, Docket No. RD09-2-000 (May 13, 2009).

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

Background
EOP-004-1 was submitted to the Commission for approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[75]

As part of EOP-004-2, on November 5, 2012, stakeholders approved the retirement of EOP-001-1 R1. EOP-004-2 was approved by the NERC Board of Trustees on November 7, 2012. Thus, EOP-001-1 R1 is presented here for informational purposes only.

EOP-009-0 R2 – Documentation of Blackstart Generating Unit Test Results

R2. The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

Background
EOP-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[76] In Order No. 749, the Commission approved the retirement of EOP-009-0 as of July 1, 2013, based on the approval of EOP-005-2, which did not carry forward R2 of EOP-009-0. Thus, EOP-009-0 R2 is presented here for informational purposes only.

FAC-008-1 R1.3.5 – Facility Ratings Methodology

R1.3.5. Other assumptions.

Background
FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[77]

"On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No.

[75] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[76] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[77] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[78]

FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[79]

FAC-008-3 (which combined FAC-008 and FAC-009) has been approved by the Commission without the "other assumptions" language.[80] Since FAC-008-3 will become effective on January 1, 2013, FAC-008-1 R1.3.5 is presented here for informational purposes only.

PRC-008-0 R1; PRC-008-0 R2 – Underfrequency Load Shedding Equipment Maintenance Programs

R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.

R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).

Background

PRC-008-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[81]

Under Standards Development Project 2007-17 Protection System Maintenance, which recently passed on August 27, 2012, PRC-008-0 is scheduled to be retired, subsumed and replaced with PRC-005-2. PRC-005-2 will likely be presented to the NERC Board of

[78] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[79] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).
[80] *Id.*

[81] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Trustees in November for approval, and, thus, PRC-008-0 is only presented here for informational purposes.

PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2 – UFLS Performance Following an Underfrequency Event

R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UFLS set points and tripping times.

R1.3. A simulation of the event.

R1.4. A summary of the findings.

R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.

Background

PRC-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[82] In Order No. 763 at paragraph 103[83] the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Thus, PRC-009-0 is presented here for informational purposes only.

[82] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[83] *Automatic Underfrequency Load Shedding and Load Shedding Plans Re-liability Standards*, 139 FERC ¶ 61,098 (2012).

TOP-001-1a R3 – Reliability Responsibilities and Authorities

R3. Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.

Background

TOP-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved by the Commission on March 16, 2007 in Order No. 693.[84] TOP-001-1a was submitted for approval on July 16, 2010 in Docket No. RM10-29-000 and was approved on September 15, 2011 in Order No. 753.[85]

IRO-001-1a R8 reads:

> Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.

Although there is redundancy between TOP-001-1a R3 and IRO-001-1a R8 as related to Reliability Coordinators, this redundancy was addressed in Standards Development Project 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces TOP-001-1a R3 and reads:

> Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued

[84] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[85] *Electric Reliability Organization Interpretation of Transmission Operations Reliability Standard*, 136 FERC ¶ 61,176, (September 15, 2011) (Order No. 753).

> and identified as such by its Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.

TOP-001-2 has been approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-001-1a R3 is presented for informational purposes only.

TOP-005-2a R1 – Operational Reliability Information

R1. As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."

Background
Without directly addressing R1 of TOP-005-1 or TOP-005-2a the Commission approved both versions of TOP-005. [86] A review of the Standards Development Project 2007-03 Real-time Transmission Operations indicates it proposes R1 of TOP-005-1 to be retired. The reasoning provided by the SDT was the following:

> Confidentiality is not a reliability issue, but a market or business issue. Since this is not a reliability issue, it does not belong in the Reliability Standards and can be deleted.[87]

As stated above, in the context of Project 2007-03, TOP-001-1a was approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-005-2a R1 is presented for informational purposes only.

[86] Order No. 693 at paragraphs 1648 through 1652 (approval of TOP-005-1); *Mandatory Reliability Standards for Interconnection Reliability Operating Limits,* 134 F.E.R.C. ¶ 61,213 (2011) (approval of TOP-005-2a).

[87] Mapping Document Project 2007-03 Real-time Operations at page 31 (April 27 2012).

Appendix A

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
BAL-005-0.2b	**R2**	√							√			H		No	No	Yes
CIP-003-3, -4	**R1.2**	√	√							√	√	L	2	No	No	Yes
CIP-003-3, -4	**R3, R3.1 R3.2 R3.3**	√	√		√					√	√	L	3	No	No	Yes
CIP-003-3, -4	**R4.2**	√	√		√				√	√	√	L	3	No	No	Yes
CIP-005-3a, -4a	**R2.6**	√	√		√					√	√	L	1	No	No	Yes
CIP-007-3, -4	**R7.3**	√	√	√							√	L	1	No	No	Yes
EOP-005-2	**R3.1**	√	√				√		√			N/A	2	No	No	Yes
FAC-002-1	**R2**	√	√	√								L	3	No	No	Yes
FAC-008-1	**R2, R3**	√	√			√		√				L	3	No	No	Yes
FAC-008-3	**R4**	√	√			√		√				L	3	No	No	Yes

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
	R5															
FAC-010-2.1	**R5****	√	√			√		√				L		No	No	Yes
FAC-011-2	**R5****	√	√			√		√				L		No	No	Yes
FAC-013-2	**R3**	√	√			√		√				L		No	No	Yes
INT-007-1	**R1.2**	√	√									L		No	No	Yes
IRO-016-1	**R2**	√	√	√								L		No	No	Yes
NUC-001-2	**R9.1** **R9.1.1** **R9.1.2** **R9.1.3** **R9.1.4**	√	√									N/A	3	No	No	Yes
PRC-010-0	**R2**	√	√	√								L		No	No	Yes
PRC-022-1	**R2**	√	√	√								L		No	No	Yes
VAR-001-2	**R5****	√							√			H	3	No	No	Yes

Paragraph 81 Project Technical White Paper

December 20, 2012

Table of Contents

I. Introduction

On March 15, 2012, the Federal Energy Regulatory Commission ("FERC" or Commission") issued an order[1] on the North American Electric Reliability Corporation's ("NERC") Find, Fix and Track ("FFT") process that stated in paragraph 81 ("P81"):

> The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the [Electric Reliability Organization] ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

A. Consensus Process

In response to P81 and the Commission's request for comments to be coordinated,[2] during June and July 2012, various industry stakeholders, Trade Associations,[3] staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria,

---

[1] *North American Electric Reliability Corporation,* 138 FERC ¶ 61,193 at P 81 (2012).

[2] In addition to addressing P81, the consensus effort was also consistent with recommendation #4 set forth in *NERC's Recommendations to Improve The Standards Development Process* at page 12 (April 2012), which states:

Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address: . . . The retirement of standards no longer needed to meet an adequate level of reliability.

[3] Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Large Public Power Council, Electricity Consumers Resource Council, The Electric Power Supply Association, and Transmission Access Policy Study Group.

and, thus, could be retired. Specifically, the three parties (industry stakeholders/Trade Associations, staff from NERC, and staff from the NERC Regions) used the following conservative discipline to arrive at the proposed list of requirements to be retired: (i) the development of criteria to determine whether a Reliability Standard requirement should be retired and (ii) the application of this criteria with consultation from Subject Matter Experts ("SME"), with the understanding that if any of the three parties objected to including a requirement it would not be included in the initial phase of the P81 Project. As a result of this process, a draft Standards Authorization Request ("SAR"), including an initial suggested list of requirements for retirement, was drafted and presented to the NERC Standards Committee. Also, the SMEs consulted in this process provided the technical justifications that appear in this technical white paper.

B. Standards Committee

On July 11, 2012, the Standards Committee authorized the draft SAR to be posted for industry comment and formed an interim P81 Standards Drafting Team ("SDT") to review and respond to comments as well as finalize the SAR. The draft SAR was posted on August 3, 2012 with stakeholder comments due on or before September 4, 2012. Based on the stakeholder comments received, the SDT finalized the SAR, including the criteria and the initial list of Reliability Standard requirements proposed for retirement. On September 28, 2012, the Standards Committee Executive Committee authorized: (a) waiving the 30 day initial comment period and (b) posting the SAR and list of requirements proposed for retirement in the initial phase for a 45-day formal comment period with the formation of a ballot pool during the first 30 days and an initial ballot during the last 10 days of that 45-day comment period.[4]

The purpose of this technical white paper is to set forth the background and technical justification for each of the Reliability Standard requirements proposed for retirement. Stakeholders are requested to review this technical white paper and provide the SDT any: (1) supplemental, additional technical justifications for a requirement(s) and/or (2) concerns with the technical justifications for a requirement(s).

[4] The following requirements that were presented in the draft SAR were already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the Board in November), and, thus, are presented in this technical white paper in Section V for informational purposes only: CIP-001-2a R4; COM-001-1.1 R6; EOP-004-1 R1; EOP-009-0 R2; FAC-008-1 R1.3.5; PRC-008-0 R1; PRC-008-0 R2; PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2; TOP-001-1a R3; and TOP-005-2a R1. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the Board of Trustees for retirement or filed with the Commission or Canadian governmental authorities as part of the P81 Project. Those requirements that were not part of the draft SAR, but were added based on stakeholder comments are denoted by a "**" throughout this technical white paper. More detail on each of these requirements is provided below.

II. Executive Summary

The SDT developed a set of three criteria and used them to identify requirements that could be eligible for retirement. A summary of the criteria are as follows:

A. Criterion A (Overarching Criterion): little, if any, benefit or protection to the reliable operation of the BES

B. Criteria B (Identifying Criteria)
   - B1. Administrative
   - B2. Data Collection/Data Retention
   - B3. Documentation
   - B4. Reporting
   - B5. Periodic Updates
   - B6. Commercial or Business Practice
   - B7. Redundant

C. Criteria C (Additional data and reference points)
   - C1. Part of a FFT filing
   - C2. Being reviewed in an ongoing Standards Development Project
   - C3. Violation Risk Factor ("VRF") of the requirement
   - C4. Tier in the 2013 Actively Monitored List ("AML")
   - C5. Negative impact on NERC's reliability principles
   - C6. Negative impact on the defense in depth protection of the BES
   - C7. Promotion of results or performance based Reliability Standards

Specifically, for a requirement to be proposed for retirement, it must satisfy both, Criterion A and at least one of the Criteria B. Criteria C were considered as additional information to make a more informed decision.

Based on the criteria above, the SDT proposes to retire the following 3~~6~~8 requirements in 23 Reliability Standard versions:

- BAL-005-0.2b R2
- ~~CIP-001-2a R4~~
- CIP-003-3 R1.2
- CIP-003-3 R3
- CIP-003-3 R3.1
- CIP-003-3 R3.2
- CIP-003-3 R3.3

- CIP-003-3 R4.2
- CIP-003-4 R1.2
- CIP-003-4 R3
- CIP-003-4 R3.1
- CIP-003-4 R3.2
- CIP-003-4 R3.3
- CIP-003-4 R4.2
- CIP-005-3a R2.6
- CIP-005-4a R2.6
- CIP-007-3 R7.3
- CIP-007-4 R7.3
- ~~EOP-004-1 R1~~
- EOP-005-2 R3.1
- FAC-002-1 R2
- FAC-008-1 R2
- FAC-008-1 R3
- FAC-008-3 R4
- FAC-008-3 R5
- FAC-010-2.1 R5**
- FAC-011-2 R5**
- FAC-013-2 R3
- INT-007-1 R1.2
- IRO-016-1 R2
- NUC-001-2 R9.1
- NUC-001-2 R9.1.1
- NUC-001-2 R9.1.2
- NUC-001-2 R9.1.3
- NUC-001-2 R9.1.4
- PRC-010-0 R2
- PRC-022-1 R2
- VAR-001-2 R5**

A table is included in Appendix A with the Reliability Standard requirements proposed for retirement and a cross-reference to the associated criteria.

III. Criteria

The P81 Project focuses on identifying FERC-approved Reliability Standard requirements that satisfy the criteria set forth below.[5] Specifically, for a Reliability

[5] The scope of future phases of the P81 Project has not yet been determined. When the scope is considered, the criteria set forth herein may be a useful guide to appropriate criteria for those phases.

Standard requirement to be proposed for retirement it must satisfy **both**: (i) Criterion A (the overarching criterion) and (ii) at least one of the Criteria B listed below (identifying criteria). The purpose of having these two levels of criteria was to confine the review and consideration of requirements to only those requirements that clearly need not be included in the mandatory Reliability Standards. Also, Criteria A and B were designed so there would be no rewriting or consolidation of requirements, and the technical merits of retiring the requirements did not require significant research and vetting. In addition, for each Reliability Standard requirement proposed for retirement, the data and reference points set forth below in Criteria C were considered to make a more informed decision on whether to proceed with retirement. Lastly, for each requirement proposed for retirement, any increase to the efficiency of the ERO compliance program is addressed.

Criterion A (Overarching Criterion)

The Reliability Standard requirement requires responsible entities ("entities") to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Section 215(a) (4) of the United States Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

Criteria B (Identifying Criteria)

B1. Administrative

The Reliability Standard requirement requires responsible entities ~~("entities")~~ to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

This criterion is designed to identify requirements that can be removed with little effect on reliability and whose removal will result in an increase in the efficiency of the ERO compliance program. Administrative functions may include a task that is or is not related to developing procedures or plans, such as establishing communication contacts. Thus, for certain requirements, Criterion B1 is closely related to Criteria B2, B3 and B4. Strictly administrative functions do not inherently negatively impact reliability directly and, where possible, should be eliminated for purposes of efficiency and to allow the ERO and entities to appropriately allocate resources.

B2. Data Collection/Data Retention

These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

This criterion is designed to identify requirements that can be removed with little effect on reliability. The collection and/or retention of data do not necessarily have a reliability benefit and yet are often required to demonstrate compliance. Where data collection and/or data retention is unnecessary for reliability purposes, such requirements should be eliminated in order to increase the efficiency of the ERO compliance program.

B3. Documentation

The Reliability Standard requirement requires responsible entities to develop a document (*e.g.*, plan, policy or procedure) which is not necessary to protect BES reliability.

This criterion is designed to identify requirements that require the development of a document that is unrelated to reliability or has no performance or results-based function. In other words, the document is required, but no execution of a reliability activity or task is associated with or required by the document.

B4. Reporting

The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there would be little reliability impact.

B5. Periodic Updates

The Reliability Standard requirement requires responsible entities to periodically update (*e.g.*, annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

This criterion is designed to identify requirements that impose an updating requirement that is out of sync with the actual operations of the BES, unnecessary or duplicative.

B6. Commercial or Business Practice

The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

This criterion is designed to identify those requirements that require: (i) implementing a best or outdated business practice or (ii) implicating the exchange of or debate on commercially sensitive information while doing little, if anything, to promote the reliable operation of the BES.

B7. Redundant

The Reliability Standard requirement is redundant with: (i) another FERC-approved Reliability Standard requirement(s); (ii) the ERO compliance and monitoring program or (iii) a governmental regulation (*e.g.*, Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

This criterion is designed to identify requirements that are redundant with other requirements and are, therefore, unnecessary. Unlike the other criteria listed in Criterion B, in the case of redundancy, the task or activity itself may contribute to a reliable BES, but it is not necessary to have two duplicative requirements on the same or similar task or activity. Such requirements can be removed with little or no effect on reliability and removal will result in an increase in efficiency of the ERO compliance program.

Criteria C (Additional data and reference points)

~~In those instances where there is a need for additional information t~~To assist in the determination of whether to proceed with the ~~a Reliability Standard~~ requirement of a Reliability Standard requirement that satisfies both Criteria A and B, the following data and reference points shall be considered to make a more informed decision:

C1. Was the Reliability Standard requirement part of a FFT filing?

The application of this criterion involves determining whether the requirement was included in a FFT filing.

C2. Is the Reliability Standard requirement being reviewed in an on-going Standards Development Project?

The application of this criterion involves determining whether the requirement proposed for retirement is part of an active on-going Standards Development Project, with a consideration of the point in the process that Project is at. If the requirement has been passed by the stakeholders and is scheduled to be presented to the NERC Board of Trustees, in most cases it will not be included in the P81 project to promote regulatory efficiency. The exception would be a requirement, such as the Critical Information Protection ("CIP") requirements for Version 3 and 4, that is not due to be retired for an extended period of time; or, other requirements that based on the specific facts and circumstances of that requirement indicate it should be retired via the P81 Project first rather than waiting for another Standards Development Project to retire it, particularly as a way to increase the efficiencies of the ERO compliance program. Also, for informational purposes, whether the requirement is included in a future or pending Standards Development Project will be identified and discussed.

C3. What is the VRF of the Reliability Standard requirement?

The application of this criterion involves identifying the VRF of the requirement proposed for retirement, with particular consideration of any requirement that has been assigned as having a Medium or High VRF. Also, the fact that a requirement has a Lower VRF is not dispositive that it qualifies for retirement. In this regard, Criterion C3 is considered in light of Criterion C5 (Reliability Principles) and C6 (Defense in Depth) to ensure that no reliability gap would be created by the retirement of the Lower VRF requirement. For example, no requirement, including a Lower VRF requirement, should be retired if its retirement harms the effectiveness of a larger scheme of requirements that are purposely designed to protect the reliable operation of the BES.

C4. In which tier of the 2013 AML does the Reliability Standard requirement fall?

The application of this criterion involves identifying whether the requirement proposed for retirement is on the 2013 AML, with particular consideration for any requirement in the first tier of the 2013 AML.

C5. Is there a possible negative impact on NERC's published and posted reliability principles?

The application of this criterion involves consideration of the eight following reliability principles published on the NERC webpage.

> **Reliability Principles**
> NERC Reliability Standards are based on certain reliability principles that define the foundation of reliability for North American bulk power systems. Each reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of reliability of the North American bulk power systems. Each reliability standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.
>
> Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

Principle 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

Principle 7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks. (footnote omitted).

C6. Is there any negative impact on the defense in depth protection of the BES?

The application of this criterion considers whether the requirement proposed for retirement is part of a defense in depth protection strategy. In order words, the assessment is to verify whether other requirements rely on the requirement proposed for retirement to protect the BES.

C7. Does the retirement promote results or performance based Reliability Standards?

The application of this criterion considers whether the requirement, if retired, will promote the initiative to implement results- and/or performance-based Reliability Standards.

IV. The Initial Phase Reliability Standards Requirements Proposed for Retirement

The following lists the requirements proposed for retirement with details of the assessment resulting from the applicability of the criteria above.

BAL-005-0.2b R2 – Automatic Generation Control

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.

Background/Commission Directives

BAL-005-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[6] Also, the Commission accepted an errata filing to BAL-005-0.1b, which replaced Appendix 1 with a corrected version of a Commission-approved interpretation, and made an internal reference correction in the interpretation, thus resulting in BAL-005-0.2b.[7]

In Order No. 693 at paragraph 387, the Commission stated that:

> The goal of this Reliability Standard is to maintain Interconnection frequency by requiring that all generation, transmission, and customer load be within the metered boundaries of a balancing authority area, and establishing the functional requirements for the balancing authority's regulation service, including its calculation of ACE.

At paragraph 396, the Commission stated:

> On this issue, the Commission directs the ERO to modify BAL-005-0 through the Reliability Standards development process to develop a process to calculate the minimum regulating reserve for a balancing authority, taking into account expected load and generation variation and transactions being ramped into or out of the balancing authority.

[6] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[7] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Errata Changes to Seven Reliability Standards, Docket No. RD12-4-000 (September 13, 2012).

This Commission directive is unaffected by the proposed retirement of BAL-005-0.2b R2.

Additionally, when adjusting the VRF for the previous version, BAL-005-0.1b R2, from Lower to High, the Commission stated that:[8]

> While theoretically, CPS can be met without the use of AGC, for example, when the AGC system is malfunctioning, the Commission believes, in practice, that AGC is the most dependable and effective means for multiple balancing authorities in an Interconnection to collectively meet CPS requirements in tandem while minimizing assistance from each other in this regard. Human reaction is neither fast enough nor dependable enough in this repetitive task to provide the immediate and continuous support to correct for Interconnection frequency drift. Further, the failure to use AGC presents a higher risk that immediate load shedding will need to be implemented after the sudden loss of generation or an unforeseen significant load increase and, thus, the failure to use AGC subjects the Bulk-Power System to a higher risk of instability.

However, the fact that the VRF for BAL-005-0.2b R2 is High is not indicative of its actual impact on the BES as explained in further detail below. Also, no Commission directive is impacted by BAL-005-0.2b R2.

Technical Justification

The stated reliability purpose of BAL-005-0.2b is to establish requirements for Balancing Authority Automatic Generation Control ("AGC") necessary to calculate Area Control Error ("ACE") and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved. The reliability purpose and objectives of BAL-005-0.2b are unaffected by the proposed retirement of R2.

A Balancing Authority must use AGC to control its Regulating Reserves to meet the Control Performance Standards ("CPS") as set forth in BAL-001-0.1a R1 and R2. Although for a short period of time (as the Commission stated during an AGC malfunction) a Balancing Authority may be able to meet its CPS obligations without AGC, it cannot do so for any extended period of time, and, therefore, Balancing Authorities must use AGC to control its Regulating Reserves to satisfy its obligations under BAL-001-0.1a R1 and R2. Given this fact, it is redundant to also have BAL-005-0.2b R2 set forth the following statement: "Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard." (Criterion B7). It is the duplicative nature of having two requirements requiring the same activity that does little, if anything, to benefit or protect reliable

[8] *North American Electric Reliability Corporation*, 121 FERC ¶ 61,179 at P 50 (2007).

operation of the BES. (Criterion A). In other words, without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a R1 and R2.

Also, the retirement of BAL-005-0.2b R2 would increase the efficiency of the ERO compliance program because NERC and the Regional Entities would be able to focus their time and resources on monitoring compliance on BAL-001-0.1a R1 and R2, which are results-based requirements, versus monitoring compliance with both BAL-001-0.1a R1 and R2 as well as the static statement in BAL-005-0.2b R2. Therefore, retiring BAL-005-0.2b R2 will provide for increased efficiencies in the ERO compliance program.

Criterion A
Without the existence of BAL-005-0.2b R2, Balancing Authorities must still have Regulating Reserves that can be controlled by AGC to satisfy the CPS in BAL-001-0.1a R1 and R2. Having two requirements requiring a Balancing Authority to conduct the same activity or task does little, if anything, to benefit or protect the reliable operation of the BES because it is duplicative.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. BAL-005-0.2b R2 has not been part of a FFT filing.

2. BAL-005-0.2b R2 is currently scheduled to be included in Standards Development Project 2010-14.2, which is Phase II of Balancing Authority Reliability-based Controls: Time Error, AGC, and Inadvertent. Given that Project 2010-14.2 is currently not an active Standards Development Project, it remains appropriate to retire BAL-005-0.2b R2 via the P81 Project.

3. The VRF for BAL-005-0.2b R2 is High. Given the redundant nature of BAL-005-0.2b R2, the High VRF is not dispositive of whether or not it should be retired since BAL-001-0.1a R1 and R2 accomplishes the important reliability requirement of Balancing Authorities maintaining Regulating Reserves that can be controlled by AGC to satisfy CPS.

4. BAL-005-0.2b R2 is not part of the 2013 AML.

5. The redundant nature of BAL-005-0.2b R2 with BAL-001-0.1a R1 and R2 also indicates that the retirement of BAL-005-0.2b R2 does not pose a negative impact to NERC's published and posted reliability principles. The two reliability principles applicable to BAL-005-0.2b R2 are the following:

Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement of BAL-005-0.2b R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. As discussed above, given that BAL-001-0.1a R1 and R2 already require that AGC be used to control Regulating Reserves, there is no risk or gap to reliability resulting from the retirement of BAL-005-0.2b R2.

7. Retirement of BAL-005-0.2b R2 promotes a results-based approach, because it is retiring a static requirement while BAL-001.1a R1 and R2, which are more dynamic and results-based requirements, will remain in effect.

Accordingly, for the above reasons, it is appropriate to retire BAL-005-0.2b R2.

~~**CIP-001-2a R4 Sabotage Reporting**~~

~~**R4.** Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.~~

~~**Background/Commission Directives**~~

~~CIP-001-1 was filed for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[9] CIP-001-1a was filed for Commission approval on April 21, 2010 in Docket No. RD10-11-000, and was approved by an unpublished letter order on February 2, 2011.[10]~~

~~CIP-001-2a was filed for Commission approval as a Regional Variance for the ERCOT Region, containing an interpretation of CIP-001-1, on June 21, 2011 in Docket No. RD11-6-000 and was approved by unpublished letter order on August 2, 2011.[11]~~

~~[9] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).~~
~~[10] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-001-1 – Cyber Security – Sabotage Reporting, Requirement R2, Docket No. RD10-11-000 (February 2, 2011).~~
~~[11] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of the Reliability Standard CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity, Docket No. RD11-6-000 (August 2, 2011).~~

In Order No. 693 at paragraph 460, the Commission stated:

> For these reasons, the Commission remains concerned that a wider application of CIP-001-1 may be appropriate for Bulk-Power System reliability. Balancing these concerns with our earlier discussion of the applicability of Reliability Standards to smaller entities, we will not direct the ERO to make any specific modification to CIP-001-1 to address applicability. However, we direct the ERO, as part of its Work Plan, to consider in the Reliability Standards development process, possible revisions to CIP-001-1 that address our concerns regarding the need for wider application of the Reliability Standard. Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.

In Order No. 693 at paragraphs 445 and 467 through 470, the Commission stated that:

> The goal of CIP-001-1 is to ensure that operating entities recognize sabotage events and inform appropriate authorities and each other to properly respond to the sabotage to minimize the impact on the Bulk-Power System. The Reliability Standard requires that each reliability coordinator, balancing authority, transmission operator, generation operator and LSE have procedures for recognizing and for making operating personnel aware of sabotage events, and communicating information concerning sabotage events to appropriate "parties" in the Interconnection.
>
> * * *
>
> CIP-001-1, Requirement R4, requires that each applicable entity establish communications contacts, as applicable, with the local FBI or Royal Canadian Mounted Police officials and develop reporting procedures as appropriate to its circumstances. The Commission in the NOPR expressed concern that the Reliability Standard does not require an applicable entity to actually contact the appropriate governmental or regulatory body in the event of sabotage. Therefore, the Commission proposed that NERC modify the Reliability Standard to require an applicable entity to "contact appropriate federal authorities, such as the Department of Homeland Security, in the event of sabotage within a specified period of time."
>
> As mentioned above, NERC and others object to the wording of the proposed directive as overly prescriptive and note that the reference to "appropriate federal authorities" fails to recognize the international application of the Reliability Standard. The example of the Department of

> Homeland Security as an "appropriate federal authority" was not intended to be an exclusive designation. Nonetheless, the Commission agrees that a reference to "federal authorities" could create confusion. Accordingly, we modify the direction in the NOPR and now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event. The ERO's Reliability Standards development process should develop the language to implement this directive.
>
> * * *
>
> Thus, the Commission directs the ERO to modify CIP-001-1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time, even if it is a preliminary report. The ERO, through its Reliability Standards development process, is directed to determine the proper reporting period. In doing so, the ERO should consider suggestions raised by commenters such as FirstEnergy and Xcel to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage, and APPA's concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities. (Footnotes omitted).

The Commission's suggestion to modify CIP-001-1 to require an applicable entity to contact appropriate federal authorities, such as the Department of Homeland Security, is being considered in Standards Development Project 2009-01 (EOP-004-2). CIP-001-2a R4 is proposed for retirement because it does not require an action when sabotage is suspected or actually occurs, rather that action is addressed via CIP-001-2a R2.

Technical Justification

The practices and procedures set forth in CIP-001-2a R2 provides the results-based foundation for contacting communication of information concerning sabotage events to appropriate parties in the Interconnection, including when necessary, the FBI or RCMP, when there is an event of suspected or actual sabotage, while the task in R4 does little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A). Consistent with CIP-001-2a R1 (identification of sabotage), R2 (communication of sabotage) and R3 (reporting of sabotage),[12] a responsible entity generally contacts local law enforcement authorities when there is any suspicion that sabotage has occurred at a BES facility. The entity's corporate security and site personnel will consult with local law enforcement to assess the situation and facts to determine whether a suspected or actual act of sabotage has occurred. If they find a suspected or actual act of sabotage has

[12] "**R2.** Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection."

occurred, the FBI or RCMP, as appropriate, will be contacted in accordance with R2.[13] Thus, pursuant to the different steps and actions in R1 through R3, when there is an instance of sabotage that warrants contacting the FBI or RCMP or any other federal/national governmental authority, the responsible entities will contact them. Conversely, CIP-001-2a R4 does not require that the FBI or RCMP be contacted when an act of suspected or actual sabotage has occurred; instead, R4 only requires that the entity establish communication contacts with these agencies, as appropriate, and "develop reporting procedures. . . ." While the development of reporting procedures in R4 is generic, the procedures and processes associated with R1, R2, and R3 are specific to the steps of identifying, communicating and reporting issues related to sabotage. This view was confirmed in the interpretation of R2 that states:

> . . . the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information.

Consequently, the R4 requirement to establish communication contacts and develop reporting procedures does not support reliability, and, instead, is an administrative, documentation and data collection task requirement (Criteria B1, B2 and B3). Also, in the overall context of CIP-001-2a R1 through R3, which already require sabotage related procedures and guidelines, the tasks in R4 are unnecessary and needlessly burdensome. Furthermore, corporate security departments that are involved in the investigation of sabotage related events are well aware of how to contact the FBI and RCMP, as applicable, and, in fact, some corporate security employees to have a law enforcement background, including past positions in federal agencies such as the Secret Service. To have these security professionals establish contacts with agencies they are readily familiar with and to generic develop reporting procedures that do not require action is unnecessarily burdensome. The administrative aspect of R4 is further illuminated when compared to the more results-based activities in CIP-001-2a R1 through R3, which are the requirements that serve reliability by requiring action when suspected or actual sabotage occurs. Accordingly, CIP-001-2a R1 through R3 serve the results-based reliability function, while R4 is a static, administrative requirement that has no direct or clear nexus to protecting BES reliability.

Also, the retirement of CIP-001-2a R4 should increase the efficiencies of the ERO compliance program, because ERO and Regional Entity time and resources would be able to focus more attention, if needed, on monitoring compliance with CIP-001-2a R1 through R3.

[13] In addition, the requirement, as written, does not reflect current reporting and investigation procedures in some of the Canadian Provinces as protocol for sabotage reporting and investigation varies in each Canadian Province. For example, in the Provinces of Ontario and Quebec, the reports are given to local police (municipal/provincial) and not to the RCMP as the standard specifies. The fact is that the RCMP does not perform Provincial level law enforcement in the Provinces of Ontario and Quebec.

~~**Criterion A**~~

~~CIP-001-2a R2 provides the results-based foundation for contacting communication of information concerning sabotage events to appropriate parties in the Interconnection, including when necessary, the FBI or RCMP, when there is an event of suspected or actual sabotage, while the task in R4 does little, if anything, to benefit or protect the reliable operation of the BES.~~

~~**Criteria B**~~

- ~~Criterion B1 (Administrative)~~
- ~~Criterion B2 (Data Collection/Data Retention)~~
- ~~Criterion B3 (Documentation)~~

~~**Criteria C**~~

1. ~~CIP-001-2a R4 has been part of a FFT filing.~~[14]

2. ~~CIP-001-2a R4 is part of an on-going Standards Development Project 2009-01 (EOP 004-2). At this time, EOP-004-2 has not been approved by stakeholders and the NERC Board of Trustees, and, therefore, it is appropriate to retain CIP-001-2a R4 within the scope of P81. However, if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 Project and may include CIP-001-2a R4 for informational purposes only.~~

3. ~~CIP-001-2a R4 has a Medium VRF. All of CIP-001-2a has a Medium VRF, thus the fact that R4 is a Medium VRF is not dispositive of whether it should be retired.~~

4. ~~CIP-001-2a R4 is in the second tier of the AML. Similar to the VRF, having CIP-001-2a R4 in the second tier of the AML is not dispositive of whether it should be retired, particularly when considered with the fact that R2 and R3, the more results-based requirements, are in the first tier.~~

5. ~~Given its lack of requiring a reliability based action, the retirement of CIP-001-2a R4 does not negatively impact NERC's published and posted reliability principles. The only principles applicable to CIP-001-2a R4 appear to be the following:~~

> ~~Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.~~

~~[14] NERC FFT Informational Filing, Docket No. RC12-15-000 (August 31, 2012); NERC FFT Informational Filing, Docket No. RC12-13-000 (June 29, 2012); NERC FFT Informational Filing, Docket No. RC12-11-000 (April 30, 2012); NERC FFT Informational Filing, Docket No. RC12-6-000 (December 30, 2011); NERC FFT Informational Filing, Docket No. RC12-2-000 (November 30, 2011); NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011); NERC FFT Informational Filing, Docket No. RC11-6-000 (September 30, 2011).~~

~~Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks.~~

~~6. The retirement of CIP-001-2a R4 does not impact a defense in depth strategy between multiple requirements. CIP-001-2a R1 through R3 provide the foundation for the identification, communication and reporting of suspected and actual sabotage, while R4 is an administrative task of establishing contacts and developing generic reporting procedures. Therefore, there is no reliability risk or gap that will result from the retirement of CIP-001-2a R4.~~

~~7. As mentioned above, CIP-001-2a R4 is not a results-based requirement.~~

~~Accordingly, for the above reasons, it is appropriate to retire CIP-001-2a R4.~~

CIP-003-3, -4 R1.2 – Cyber Security – Security Management Controls

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[15] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[16] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[17] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[18]

In Order No. 706 at paragraph 342 the Commission stated that:

> Reliability Standard CIP-003-1 seeks to ensure that each responsible entity has minimum security management controls in place to protect the critical

[15] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).
[16] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[17] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[18] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

> cyber assets identified pursuant to CIP-002-1. To achieve this goal, a responsible entity must develop a cyber security policy that represents management's commitment and ability to secure its critical cyber assets. It also must designate a senior manager to direct the cyber security program and to approve any exception to the policy.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R1.2 does not impact a Commission directive.

Technical Justification

The importance of the cyber security policy as representing management's commitment and ability to secure critical cyber assets is overshadowed by the rigorous and specific training, procedural and process related requirements of the CIP Standards. These trainings, procedures and processes render having the cyber security policy readily available an unnecessary requirement. In other words, whether CIP personnel are completing a typical CIP requirement cyber security task or responding to an immediate situation, they will act via their specific training, processes and procedures and not the overarching cyber security policy. Stated another way, CIP personnel will act via their specific training, processes and procedures which reflect the overarching cyber security policy. Consequently, the cyber security policy's generalized guidance on compliance with the CIP requirements is not a document that adds value to personnel protecting the BES from a cyber attack on a day-to-day basis.

Furthermore, to implement CIP-003-3, -4 R1.2 entities have undertaken a variety of administrative solutions including kiosks dedicated to computers with the cyber security policy, posting the policy on the company intranet, having copies available in work stations, at common area desks in generating stations and substations, etc. Therefore, although the cyber security policy is readily available for all personnel who have access to, or are responsible for, Critical Cyber Assets, these personnel are specifically and appropriately focused on implementing the procedures and processes required by CIP Reliability Standards such as CIP-007-3 R1, which states as follows:

> Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

Generally the cyber security policy will cite CIP-007-3 R1 as a requirement, and may refer to procedures related to CIP-007-3 R1, but will not have, nor is it required to have, the detail necessary to implement CIP-007-3 R1. In some larger companies, it is also

common to have specific procedures on how to accomplish requirements such as CIP-007-3 R1 in a control center versus a generating plant or substation, and it may be different CIP personnel implementing these procedures in locations many hundreds of miles, states or Interconnections away from each other. The value of a more general cyber security policy to these individuals is minimal, at best, and, therefore, does not support reliability. Also, making it readily available at all office locations is an unnecessarily burdensome administrative task.

Moreover, to place every procedure and process to comply with CIP in the cyber security policy is also not practical or effective, because such a large policy will only distract from CIP personnel being able to specifically focus on the task before them. As already stated, there are likely some differences between implementing a requirement like CIP-007-1 R1 in a control center that may be located in one state and for generators located several states and hundreds of miles away. Thus, making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES (Criteria A and B1).

In this context, also consider the inefficiencies CIP-003-3, -4 R1.2 may be causing the ERO compliance program. In companies with hundreds of personnel who have access to, or are responsible for, Critical Cyber Assets in multiple states and Interconnections, the ERO may expend a significant amount of time and resources to monitor compliance with CIP-003-3, -4 R1.2 via a review of kiosks, intranet sites, office cubicles, desks, etc in multiple locations. Accordingly, considerable efficiency gains will be obtained for the ERO's compliance program if CIP-003-3, -4 R1.2 is retired.

Criterion A
Making the cyber security policy readily available is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. CIP-003-3, -4 R1.2 has been part of a FFT filing.[19]

2. As is the case with all the CIP requirements (other than CIP-001-2a R4) proposed for retirement in this technical paper, CIP-003-3, -4 R1.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security) ("CIP V5"). The P81 SDT has coordinated its efforts with the chair of Project 2008-06. There is no conflict between CIP requirements proposed in this technical white paper for retirement and the direction of Project 2008-06. The CIP V5 requirements are not Board of Trustee or Commission approved, and, even if they were, the effective date of CIP V5 is unknown and likely at least a year, maybe more, into the future.

[19] NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

Thus, unlike the other requirements presented here for informational purposes, it is appropriate to maintain all the CIP requirements discussed in this technical paper within the scope of the P81 Project to secure the efficiency gains resulting to the ERO compliance program from their retirement.

3. CIP-003-3, -4 R1~~4~~.2 has a Lower VRF. As explained above, CIP-003-3, -4 R1~~4~~.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-003-3,-4 R1.2 is in the second tier of the AML. As explained above, CIP-003-3, -4 R1~~4~~.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given its administrative nature, CIP-003-3, -4 R1.2 does not negatively impact NERC's published and posted reliability principles. The two reliability principles that appear applicable to CIP-003-3, -4 R1.2 are the following:

   Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

   Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks.

   As stated above, other CIP requirements are replete with the requirements that CIP personnel implement to protect the BES from cyber attacks.

6. Retiring CIP-003-3, -4 R1.2 does not negatively impact defense in depth because no other requirement depends on the cyber security policy being readily available. Therefore, the removal of CIP-003,-3,-4 R1.2 cannot have a negative impact on defense in depth.

7. Retirement of CIP-003-3, -4 R1.2 promotes a results-based approach because the requirement is mechanistic and administrative, and does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R1.2.

CIP-003-3, -4 R3, R3.1, R3.2, R3.3 – Cyber Security – Security Management Controls

R3. Exceptions – Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Background/Commission Directives

CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[20] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[21] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[22] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[23]

In Order No. 706 at paragraphs 373 and 376 the Commission stated that:

> Requirement R3 provides that a responsible entity must document exceptions to its policy with documentation and senior management approval. The Commission is concerned that, if exceptions mount, there would come a point where the exceptions rather than the rule prevail. In such a situation, it is questionable whether the responsible entity is actually implementing a security policy. We therefore believe that the Regional Entities should perform an oversight role in providing accountability of a responsible entity that excepts itself from compliance with the provisions of its cyber security policy. Further, we believe that

[20] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, order on clarification, Order No. 706-C, 127 FERC ¶ 61,273 (2009).
[21] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[22] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[23] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

> such oversight would impose a limited additional burden on a responsible entity because Requirement R3 currently requires documentation of exceptions.
>
> Further, the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 do not impact a Commission directive.

Technical Justification

CIP-003-3, -4 R3, R3.1, R3.2, and R3.3 (CIP exception requirements) have proven not to be useful and have been subject to misinterpretation. For instance, although the CIP exception requirements have not been available for use to exempt an entity from compliance with any requirement of any Reliability Standard, based on questions received by NERC CIP Staff, entities may be interpreting the CIP exception requirements to allow for such an exemption. The CIP exception requirements only apply to exceptions to internal corporate policy, and only in cases where the policy exceeds a Reliability Standard requirement or addresses an issue that is not covered in a Reliability Standard. For example, if an internal corporate policy statement requires that all passwords be a minimum of eight characters in length, and be changed every 30 days, which is over and above what is required in CIP-007-3 R5.3, the CIP exception requirements could be invoked for internal governance purposes to lessen the corporate requirement back to the password requirements in CIP-007-3 R5.3, but under no circumstances do the CIP exception requirements authorize the implementation of security measures less than what is required in CIP-007-3 R5.3.

The retirement of the CIP exception requirements would not impact an entity's ability to maintain such an exception process within their corporate policy governance procedures, if it so desired. Consequently, the CIP exception requirements were always an internal administrative and documentation requirement that is outside the scope of the other CIP requirements (Criteria B1 and B3). In this context, the CIP exception requirements do not support the level of reliability set forth in the Reliability Standards, and are unnecessarily burdensome because they have resulted in entities implementing practices due to a misinterpretation of the requirement that has caused them to allocate time and resources to tasks that are misaligned with the requirements themselves. Unfortunately, this misunderstanding has also impacted the efficiency of the ERO compliance program because of the amount of time and resources needed to clear up the misunderstanding and

coach entities on the meaning of the CIP exception requirements. These inefficiencies would be eliminated with the retirement of the CIP exception requirements. Accordingly, as explained, the CIP exception requirements are an administrative tool for internal corporate governance procedures, and, therefore, are not requirements that are necessary or directly protect the BES from a cyber attack, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A).

Criterion A
The CIP exception requirements are a tool for internal corporate governance procedures and is not a requirement directly protecting the BES from a cyber attack, and, therefore, the tasks associated with these requirements do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C

1. The CIP exception requirements have been part of a FFT filing.[24]

2. The CIP exception requirements are part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between the CIP exception requirements proposed in this technical white paper for retirement and the direction of Project 2008-06.

3. The CIP exception requirements each have a Lower VRF. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. The CIP exception requirements are on the third tier of the AML. As explained above, they are not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the administrative and unnecessary nature of the CIP exception requirements in relation to protecting the BES from cyber attacks, retirement does not pose any negative impact to NERC's published and posted reliability principles, of which only Principle 8 appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

[24] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-6-000 (December 30, 2011).

6. Retiring the CIP exception requirements does not negatively impact any defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of the CIP exception requirements promotes a results-based approach because the CIP exception requirements are approaches that entities may voluntarily take to handle internal corporate governance procedures, and, therefore, do not provide the foundation for performing a required reliability task.

Accordingly, for the above reasons, it is appropriate to retire the following CIP exception requirements: CIP-003-3, -4 R3, R3.1, R3.2, and R3.3.

CIP-003-3, -4 R4.2 - Cyber Security – Security Management Controls

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Background/Commission Directives
CIP-003-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[25] CIP-003-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[26] CIP-003-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[27] CIP-003-4 was submitted for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[28] In Order No. 706, the Commission did not specifically address CIP-003-3, -4 R4.2.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-003-3, -4 R4.2 does not impact a Commission directive.

Technical Justification
The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an unnecessarily administrative and a documentation task that is redundant with CIP-003-3, -4 R4 (Criteria A, B1, B3 and B7). Specifically, CIP-003-3, -4 R4[29] already requires the classification of

[25] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[26] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[27] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[28] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, (2012).
[29] "**R4**. Information Protection — The Responsible Entity shall implement and document a program to

information associated with Critical Cyber Assets. The only difference between R4 and R4.2 is that the subjective term "based on the sensitivity" has been added, thus, making it essentially redundant. Further, CIP-003-3, -4 R4 ~~since~~ requires the entity to develop classifications based on a subjective understanding of sensitivity (*i.e.*, no clear connection to serving reliability), the requirement does not support reliability. In this context, classifying based on sensitivity becomes an administrative task that becomes necessarily burdensome, because of all the possible ramifications "based on sensitivity" can produce, and, therefore, require SMEs to decide on and reduce to writing in a documented program. This is time and effort that could be better spent on other CIP activities that provide value to cyber security and actively protect the BES. For similar reasons, retiring CIP-003-3, -4 R4.2 and the term "based on sensitivity" would increase the efficiencies of the ERO compliance program on several levels. The ERO would not spend time and resources on reviewing whether an entity's documentation contained classifications "based on sensitivity," and, instead would be able to focus its time and resources monitoring compliance with the entity's program to identify, classify, and protect information associated with Critical Cyber Assets (R4), without any distraction on monitoring the subjective implementation of classifications based on sensitivity (R4.2).

Criterion A

The task of classifying Critical Cyber Information "based on the sensitivity" does little, if anything, to benefit or protect the reliable operation of the BES, and is an administrative and a documentation task that is redundant with CIP-003-3, -4 R4.

Criteria B

- Criterion B1 (Administrative)
- Criterion B3 (Documentation)
- Criterion B7 (Redundant)

Criteria C

1. CIP-003-3, -4 R4.2 has been part of a FFT filing.[30]

2. CIP-003-3, -4 R4.2 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-003-3, -4 R4.2 and the direction of Project 2008-06.

3. CIP-003-3, -4 R4.2 has a Lower VRF. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

---

identify, classify, and protect information associated with Critical Cyber Assets."

[30] NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012); NERC FFT Informational Filing, Docket No. RC12-1-000 (October 31, 2011).

4. CIP-003-3, -4 R4.2 is on the third tier of the AML. As explained above, CIP-003-3, -4 R4.2 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

5. Given the unnecessary and redundant nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8 which appears to apply: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. Retirement of CIP-003-3, -4 R4.2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. Retirement of CIP-003-3, -4 R4.2 promotes a results-based approach because retiring CIP-003-3, -4 R4.2 moves away from prescriptive, checklist of documentation approach to Reliability Standard requirements.

Accordingly, for the above reasons, it is appropriate to retire CIP-003-3, -4 R4.2.

CIP-005-3a, -4a R2.6 – Cyber Security – Electronic Security Perimeter(s)

R2.6. Appropriate Use Banner -- Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

Background/Commission Directives

CIP-005-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[31] CIP-005-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RD09-7-000 and RM06-22-000 and was approved on September 30, 2009.[32] CIP-005-2a was filed for Commission approval on April 21, 2010 in Docket No. RD10-12-000 and was approved by unpublished letter order on February 2, 2011.[33] CIP-005-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[34] CIP-005-3a was filed for Commission approval on April 21, 2010 in Docket

[31] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[32] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[33] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).
[34] *Order on Compliance* 130 FERC ¶ 61,271 (2010).

No. RD10-12-000 and was approved by an unpublished letter order on February 2, 2011.[35] CIP-005-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No. 761.[36] CIP-005-4a was filed for Commission approval as errata to the CIP Version 4 Petition on April 12, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012 in Order No 761, the Final Rule on the CIP Version 4 standards.[37]

In Order 706 at paragraph 505 the Commission noted that:

> Requirement R2 of CIP-005-1 requires a responsible entity to implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter.

All outstanding directives in Order No. 706 will be addressed in Version 5 of the CIP Standards and the retirement of CIP-005-3, -4 R2.6 does not impact a Commission directive.

Technical Justification

The implementation of an appropriate use banner ("banner") on a user's screen for all interactive access attempts into the Electronic Security Perimeter ("ESP") is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES. Specifically, the banner does not support reliability because people who intend to inappropriately use sites will simply ignore the banner. (Criterion A). The banner is also ~~is~~ an administrative task since it simply requires a message be displayed on an access screen. Furthermore, the implementation and administration of a non-beneficial tool, such as the banner, therefore creates a needlessly burdensome task. As mentioned, above, the ineffectiveness of the banner also indicates that it does not support reliability. (Criteria B1 and B3). In addition, banners of this type are generally considered to be a form of legal protection or mitigation of liability, rather than security protection. Furthermore, the banner does not ensure a proper or secure access point configuration which is generally the purpose of CIP-005-3a, -4a. Further, this requirement has also been the subject of numerous TFEs for devices that cannot support such a banner, and hence has diverted resources from more productive efforts. Thus, the ERO's compliance program would become more efficient if CIP-005-3a, -4a R2.6 was retired, because ERO time and resources could be reallocated to monitor compliance with the remainder of CIP-005-3a, -4a, which provides for more effective controls of electronic access at all electronic access points into the ESP.

---

[35] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-005-1, Cyber Security, Electronic Security Perimeter(s), Section 4.2.2 and Requirement R1.3., Docket RD10-12-000, (February 2, 2011).

[36] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

[37] *Id.*

Criterion A
The implementation of an appropriate use banner on a user's screen for all interactive access attempts into the ESP is an activity or task that does little, if anything, to benefit or protect reliable operation of the BES, because it is administrative and a static electronic message that is not an effective deterrent or control against unauthorized access.

Criteria B
- Criterion B1 (Administrative)
- Criterion B3 (Documentation)

Criteria C
1. CIP-005-3a, -4a R2.6 has been part of a FFT filing.[38]

2. CIP-005-3a, -4a R2.6 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-005-3a, -4a R2.6 and the direction of Project 2008-06.

3. The VRF for CIP-005-3a, -4a R2.6 is Lower. As explained above, CIP-005-3a, -4a R2.6 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-005-3a, -4a R2.6 is on the first tier of the AML; however, given its clear ineffective nature the placement on the first tier is not dispositive of whether it should be retired.

5. Reliability principle No. 8 – "Bulk power systems shall be protected from malicious physical or cyber attacks" – is not implicated or negatively impacted by the retirement of CIP-005-3a, -4a R2.6, because it is not an effective deterrent or control to unauthorized access into an ESP.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. Furthermore, the remainder of CIP-005-3a, -4a provides for actual controls of electronic access at all electronic access points which addresses the reliability risk associated with unauthorized access into an ESP.

7. Its retirement also promotes a results-based approach because CIP-005-3a, -4a R2.6 is an ineffective administrative task, and, therefore, does not provide the foundation for performing a reliability task.

[38] NERC FFT Informational Filing, Docket No. RC12-13-000 (June 29, 2012); NERC FFT Informational Filing, Docket No. RC12-7-000 (January 31, 2012).

Accordingly, for the above reasons, it is appropriate to retire CIP-005-3a, -4a R2.6.

CIP-007-3, -4 R7.3 – Cyber Security – Systems Security Management

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Background/Commission Directives

CIP-007-1 was filed for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on January 18, 2008 in Order No. 706.[39] CIP-007-2 was filed for Commission approval on May 22, 2009 in Docket Nos. RM06-22-000 and RD09-7-000 and was approved on September 30, 2009.[40] CIP-007-2a was filed for Commission approval on November 17, 2009 in Docket No. RD10-3-000 and was approved on March 18, 2010.[41] CIP-007-3 was filed for Commission approval on December 29, 2009 in Docket No. RD09-7-002 and was approved on March 31, 2010.[42] CIP-007-4 was filed for Commission approval on February 10, 2011 in Docket No. RM11-11-000 and was approved on April 19, 2012.[43]

In Order No. 706 at paragraph 631 the Commission stated that:

> Requirement R7 of CIP-007-1 requires the responsible entity to establish formal methods, processes and procedures for disposal or redeployment of cyber assets. In the CIP NOPR, the Commission addressed the concern that solely to "erase the data," as stated several times in Requirement R7, may not be adequate because technology exists that allows retrieval of "erased" data from storage devices, and that effective protection requires discarded or redeployed assets to undergo high quality degaussing. We noted that erasure is as much a method as it is a goal, and that the requirement ultimately needs to assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. Degaussing is not the sole means for achieving this goal. The Commission therefore proposed to direct the ERO to modify Requirement R7 to clarify this point. (Footnote omitted)

[39] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) ("Order No. 706").
[40] *Order Approving Revised Reliability Standard for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards)).
[41] Order Approving Reliability Standard Interpretation, 130 FERC ¶ 61,184 (2010).
[42] *Order on Compliance* 130 FERC ¶ 61,271 (2010).
[43] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

This Commission directive is unaffected by the retirement of CIP-007-3,-4 R7.3 as explained below.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. [44] CIP-007-3, -4 R7.3 requires the maintaining of records for the purpose of demonstrating compliance with disposing of or redeploying of Cyber Assets in accordance with documented procedures. NERC and the Regions Entities, however, under Section 400 already have the ability to require the production of records to demonstrate compliance, thus it is unnecessary to also state the same in CIP-007-3, -4 R7.3. The maintaining of records is an administrative task, not a task directly related to the protection of the BES from a cyber attack. The maintaining of records is not a task that by itself, or in conjunction with other requirements, supports reliability. Also, the maintaining of the records becomes unnecessarily burdensome in that it requires all records be maintained, which may or may not be necessary to demonstrate compliance via the production of information under Section 400. (Criteria B1 and B2). As mentioned, CIP-007-3, -4 R7.3 does not promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A).

In contrast, the remaining substantive requirements in R7 read as follows:

> R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.
>
> R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

[44] Section 401 of NERC's Rules of Procedure provide for collection of data and information necessary to monitor compliance outside the context of Reliability Standards:

> **Data Access** — All Bulk Power System owners, operators, and users shall provide to NERC and the applicable Regional Entity such information as is necessary to monitor compliance with the Reliability Standards. NERC and the applicable Regional Entity will define the data retention and reporting requirements in the Reliability Standards *and compliance reporting procedures.* (emphasis added).

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

An entity's following of these requirements may help to protect BES reliability, but the retention of evidence associated with these requirements does not. Hypothetically, an entity could perform R7, R7.1 and R7.2 flawlessly and protect the BES, but not have any record of it. While this situation may impact a demonstration of compliance, the lack of records does not necessarily directly impact the reliability of the BES or protect it from a cyber attack.

Also, there are some inherent inefficiencies resulting from a small number of Reliability Standard requirements explicitly mandating the collection of data, evidence and records, while most data and information is collected for ERO compliance monitoring purposes without specific data collection language ~~outside the context of~~ in the Reliability Standards. In this regard, for the ERO, Regional Entities and the entities, ~~arguably~~ Reliability Standards are arguably more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A

CIP-007-3, -4 R7.3 does not promote reliability because it does not protect the BES from a cyber attack, instead it is a record retention activity. Therefore, CIP-007-3, -4 R7.3 requires an activity or task that in and of itself, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. CIP-007-3, -4 R7.3 has not been part of a FFT filing.

2. CIP-007-3, -4 R7.3 is part of an on-going Standards Development Project 2008-06 (Cyber Security). As detailed in the discussion of CIP-003-3, -4 R1.2, the P81 SDT has coordinated its efforts with the chair of Project 2008-06 and there is no conflict between retirement of CIP-007-3, -4 R7.3 and the direction of Project 2008-06.

3. The VRF for CIP-007-3, -4 R7.3 is Lower. As explained above, CIP-007-3, -4 R7.3 is not an important part of a scheme of CIP requirements, and, therefore, it is appropriate to propose it for retirement.

4. CIP-007-3, -4 R7.3 is on the first tier of the AML; however, given that it is simply requiring the retention of records the fact that is on the first tier is not dispositive of whether it should be retired.

5. Given the administrative, data collection nature of this requirement, retirement does not pose any negative impact to NERC's published and posted reliability principle No. 8: "Bulk power systems shall be protected from malicious physical or cyber attacks."

6. The retirement does not negatively impact defense in depth because data retention in-and-of-itself is not an activity that other requirements depend on to help cover a reliability gap or risk to reliability.

7. Its retirement promotes a results-based approach because the data collection/retention does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire CIP-007-3, -4 R7.3.

~~**EOP-004-1 R1 – Disturbance Reporting**~~

~~**R1.** Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.~~

~~**Background/Commission Directives**~~

~~EOP-004-1 was submitted to the Commission for approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[45] Although the Commission did not address EOP-004-1 R1 directly, in Order No. 693 at paragraph 617 it stated that EOP-004-1:~~

> ~~. . . serves an important purpose in establishing requirements for reporting and analysis of system disturbances. Accordingly, the Commission approves Reliability Standard EOP-004-1 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission directs the ERO to develop a modification to EOP-004-1 through the Reliability Standards development process that includes any Requirements necessary for users, owners and operators of the Bulk-Power System to provide data that will assist NERC in the investigation of a blackout or disturbance.~~

~~[45] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).~~

~~The directive to provide data that will assist NERC in the investigation of a blackout or disturbance is not affected by the EOP-004-1 R1, because that is accomplished via other requirements in EOP-004-1 and is also under consideration for enhancement in the development of EOP-004-2.~~

~~**Technical Justification**~~

~~The reliability purpose of EOP-004-1 is to ensure that disturbances or unusual occurrences that jeopardize the operation of the BES, or result in system equipment damage or customer interruptions, are studied and understood in order to minimize the likelihood of similar events in the future. The reliability purpose of EOP-004-1 is unaffected by the proposed retirement of R1.~~

~~EOP-004-1 R1 is an anomaly in the Reliability Standards, given that it requires the Regional Reliability Organization to develop a reporting procedure. Although the development of such a reporting procedure may be helpful guidance to responsible entities on reporting of disturbances to Regional Entities, in and of itself is an administrative and documentation task that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B3). It is worth noting that EOP-004-1 R1, like CIP-001-2a R4, is administrative in that it only requires the development of procedures, it does not require that they be followed. More importantly, the mandatory processes for reporting preliminary and final disturbance reports are set forth in EOP-004-1 R3 and its sub-requirements which read as follows:~~

> ~~R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.~~
>
> ~~R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.~~
>
> ~~R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2- EOP-004.~~
>
> ~~R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator~~

Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

There is no reliability gap created by the passive retirement of EOP-004-1 R1, because EOP-004-1 R3 and its sub-requirements require considerable action to report on disturbances.[46] Also, consider that the EOP-004-1 R1 regional procedures may take the lead from NERC, and, therefore, the regional procedures become a reiteration or a hybrid of mandatory (EOP-004-1 R3 and its sub-requirements) and voluntary rules (NERC Event Analysis Process).[47] It is an unnecessarily burdensome task to require such reiterations of NERC reporting requirements on a regional level. Also, if there was a need for particular regional procedures such procedures could exist as guidance even without the existence of EOP-004-1 R1. Thus, the value of EOP-004-1 R1 as a Reliability Standard requirement to support reliability is diminutive.

Furthermore, the retirement of EOP-004-1 R1 will increase the efficiency of the ERO compliance program in that the time and resources spent monitoring EOP-004-1 and checking off whether or not a Regional Entity has the specified procedure, and can be utilized to focus attention on an entity's compliance with EOP-004-1 R3 and its sub-requirements, which produce the information related to disturbances.

Criterion A

A requirement that Regional Entities develop a reporting procedure in and of itself is an administrative and documentation task that does little, if anything, to benefit or protect the reliable operation of the BES.

[46] While not dispositive, the NERC voluntary event analysis process is also being used to report and analyze events. A link to NERC's event analysis process is http://www.nerc.com/page.php?cid=5|365.

[47] *See, e.g.*, FRCC Disturbance Reporting Procedure, FRCC – RE – OP – 001-0 Effective Date – February 10, 2012.

~~**Criteria B**~~

- ~~Criterion B1 (Administrative)~~
- ~~Criterion B3 (Documentation)~~

~~**Criteria C**~~

~~1. EOP-004-1 R1 has not been part of a FFT filing.~~

~~2. EOP-004-1 R1 is part of an on-going Standards Development Project 2009-01 (EOP-004-2) and is being proposed for retirement as unnecessary. At this time, EOP-004-2 has not been approved by stakeholders and the NERC Board of Trustees, and, therefore, it is appropriate to retain EOP-004-1 R1 within the scope of the P81 Project. However, if EOP-004-2 does receive stakeholder approval and is adopted by the NERC Board of Trustees, the SDT will reconsider retirement via the P81 Project and may include EOP-004-1 R1 for informational purposes only.~~

~~3. The VRF for EOP-004-1 R1 is Lower.~~

~~4. EOP-004-1 R1 is in the third tier of the AML.~~

~~5. The retirement of EOP-004-1 R1 does not pose any negative impact to NERC's published and posted reliability principles, as none of the principles are directly implicated.~~

~~6. The retirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.~~

~~7. The retirement of EOP-004-1 R1 promotes a results-based approach because the requirement is an administrative task of developing a procedure with no associated actionable performance of a task that impacts reliability.~~

~~Accordingly, for the above reasons, it is appropriate to retire EOP-004-1 R1.~~

EOP-005-2 R3.1– System Restoration from Blackstart Resources

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.

Background/Commission Directives

EOP-005-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[48] EOP-005-2 was submitted for Commission approval on December 31, 2009 in Docket No. RM10-16-000 and was approved on March 17, 2011 in Order No. 749.[49] Although the Commission did not address EOP-005-2 R3 directly in Order No. 749, it stated at paragraph 17 the following:

> EOP-005-2 and EOP-006-2 clarify the responsibilities of the reliability coordinator and transmission operator in the restoration process and restoration planning and address the Commission's directives in Order No. 693 related to the EOP Standards. By enhancing the rigor of the restoration planning process, the Reliability Standards represent an improvement from the current Standards and will improve the reliability of the Bulk-Power System. The Commission is not directing any modifications to the three new Reliability Standards. Nevertheless, as discussed below, commenters raised several issues for consideration, at the time these standards are next revisited, which we believe could improve these new Reliability Standards

There are no outstanding Commission directives that are affected by the proposed retirement of EOP-005-2 R3.1.

Technical Justification

The reliability purpose of EOP-005-2 is to ensure that plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure that reliability is maintained during restoration and priority is placed on restoring the Interconnection. This reliability purpose is unaffected by the proposed retirement of R3.1.

A review of EOP-005-2 R3.1 indicates that this requirement is redundant with EOP-005-2 R3 and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1, B5 and B7). The primary reason EOP-005-2 R3.1 is unnecessary is that EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes. EOP-005-2 R3 reads:

> Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule.

---

[48] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 (2007).

[49] *System Restoration Reliability Standards*, 134 FERC ¶ 61,215, (March 17, 2011) ("Order No. 749"), *order on clarification*, 136 FERC ¶ 61,030 ("Order No. 749-A") (2011).

Consequently, since R3 requires the Transmission Operator to submit its restoration plan to the Reliability Coordinator whether or not there has been a change, R3.1 only adds a separate, duplicative administrative burden for the entity to also confirm that there were no changes based upon another pre-determined schedule. While R3.1 may have attempted to capture the likelihood that unless there have been significant changes to the entity's BES, there would be no change to the restoration plan, this is an insufficient reason to impose a needlessly burdensome, duplicative administrative requirement relative to the language in R3. EOP-005-2 R3.1 is also clearly needlessly burdensome if one considers that the time and resources of Transmission Operators is better spent reliably operating the BES, rather than submitting paperwork to a Reliability Coordinator on possibly two different pre-determined schedules – one for changes and one for no changes. For these reasons, there is no reliability gap resulting from the retirement of EOP-005-2 R3.1 because Transmission Operators already have an obligation to review and provide its restoration plan annually on a mutually agreed predetermined schedule to its Reliability Coordinator. It could also be argued that a reason for both R3 and R3.1 is for the Reliability Coordinator to organize the Transmission Operator submittals into changes versus no changes. However, with the requirement to annually review restoration plans comes the need to demonstrate and track annual reviews via the revision history index, for example, which quickly shows the Reliability Coordinator when changes have and have not occurred.

The retirement of EOP-005-2 R3.1 would also increase the efficiencies of the ERO compliance program because the ERO would be able to focus its time and resources on R3 which already captures R3.1 and not be concerned with tracking the submission of restoration plans on multiple pre-determined schedules, some with changes and some without changes. Instead, the focus of the ERO compliance program would be on whether the Transmission Operators annually submitted its restoration plan to its Reliability Coordinator on one pre-determined schedule. Thus, the retirement of EOP-005-2 R3.1 appears to benefit the ERO compliance program.

Criterion A
EOP-005-2 R3.1 is redundant and a duplicative administrative update that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B5 (Periodic Updates)
- Criterion B7 (Redundant)

Criteria C

1. EOP-005-2 R3.1 has not been part of a FFT filing.

2. EOP-005-2 R3.1 is not part of an on-going Standards Development Project.

3. EOP-005-2 R3.1 does not yet have a FERC-approved VRF.

4. EOP-005-2 R3.1 is on the second tier of the AML; however, the duplicative nature of R3 and R3.1 discounts any indication that R3.1 being in the second tier is a reason not to proceed with its retirement.

5. Since EOP-005-2 R3 already requires the Transmission Operator to submit its restoration plan to its Reliability Coordinator whether or not the plan includes changes, retirement of EOP-005-2 R3.1 does not pose any negative impact to the following of NERC's published and posted reliability principles that appear to apply:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

6. Retirement of EOP-005-2 R3.1 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of EOP-005-2 R3.1 promotes a results-based approach because the requirement is administrative and unnecessary, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire EOP-005-2 R3.1.

FAC-002-1 R2 – Coordination of Plans for New Facilities

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

Background/Commission Directives
FAC-002-0 was submitted to the Commission for approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[50] FAC-002-1 was submitted for Commission approval on September 9, 2010 in Docket No. RD10-15-000 and was approved on January 10, 2011.[51] When approving FAC-002-0 in Order No. 693 at paragraphs 692 and 693, and FAC-002-1 in a subsequent order,[52] the Commission did not directly address R2.

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-002-1 R2.

Technical Justification
Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, without the existence of FAC-002-1 R2, a Regional Entity or NERC has the ability to request and receive "documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems)." This generally would occur during a spot check or compliance audit where entities have the obligation to provide documentation sufficient to demonstrate compliance. In this regard, entities already have the obligation to produce the same information required in R2 to demonstrate compliance to R1 and its sub-requirements, thus making R2 unnecessary. To have a Reliability Standard requirement that is setting forth a data retention requirement and a requirement for the entity to deliver, upon request, that data to NERC or a Regional Entity is unnecessary and also repetitive with the NERC Rules of Procedure. Accordingly, retiring FAC-002-1 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. Thus, FAC-002-1 R2 is not necessary to support reliability. Consequently, a review of R2 indicates that it is an administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). The compilation of three years of data is a burdensome task, particularly when one considers the resources and time spent on stockpiling this information is better spent coordinating the studies, executing an interconnection agreement and ensuring that interconnections are safely and reliably energized, maintained and operated. Also, there are some inherent inefficiencies that result from a small number of requirements, such as CIP-007-3, -4 R7.3 and FAC-002-1 R2 being data, evidence and record retention requirements, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach

[50] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[51] NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2 RD10-15-000 (January 10, 2011).
[52] *North American Electric Reliability Corporation*, 134 FERC ¶ 61,015 (2011).

(typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A

A review of FAC-002-1 R2 indicates that it is an administrative and data collection requirement that does little, if anything, to benefit or protect reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. FAC-002-1 R2 has not been part of a FFT filing.

2. FAC-002-1 R2 is subject to a future Project 2010-02 Connecting New Facilities to the Grid (a review of FAC-001 and FAC-002) that is scheduled to begin in the second quarter of 2015. It seems appropriate to retire FAC-002-1 R2 at this time as it may also make the review of FAC-001 and FAC-002 more effective and efficient.

3. FAC-002-1 R2 has a Lower VRF.

4. FAC-002-1 R2 is in the third tier of the AML.

5. The retirement of FAC-002-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since there are no directly applicable reliability principles.

6. The retirement does not negatively impact defense in depth because the compilation of studies for three years has no operational or planning relationship with any other requirement.

7. The retirement of FAC-002-1 R2 promotes a results-based approach since the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-002-1 R2.

FAC-008-1 R2; FAC-008-1 R3;[53] - Facility Ratings Methodology

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.

Background/Commission Directives

FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[54]

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-1 R2 and R3.

Technical Justification

FAC-008-1 R2 and R3 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-1 R2 and R3 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-1 regarding their

[53] Unlike the other requirements presented for informational purposes only, FAC-008-1 R2 and FAC-008-1 R3 have been maintained within the scope of P81 given that they are essentially identical to FAC-008-3 R4~~;~~ and FAC-008-3 R5 ~~which are due be effective on January 1, 2013~~. Inclusion would also appear to be consistent with increasing ERO compliance program efficiencies~~, given that retirement would exempt these requirements from being included in spot checks or compliance audits that are backward looking via FAC-008-1 R2 and R3~~. FAC-008-1 R2 and FAC-008-1 R3 became inactive on December 31, 2012, due to FAC-008-3 becoming enforceable on January 1, 2013.

[54] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

facility rating methodologies whether or not the exchange envisioned by FAC-008-1 R2 and R3 occurs. Furthermore, neither FAC-008-1 R2 and R3 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-1 R2 and R3 are designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its generator step up ("GSU") transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, operating conditions, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of System Operating Limits ("SOLs"), Interconnection Reliability Operating Limits ("IROLs"), calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-1 R2 (available for inspection) and R3 (comment and responsive comments).[55] Accordingly, the requirements in FAC-008-1 R2 and FAC-008-1 R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange of comments and compliance with the substantive requirements of FAC-008-1. Instead of spending time and resources on FAC-008-1 R2 and R3, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-1.

Criterion A

[55] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-02 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element.

The requirements in FAC-008-1 R2 and R3 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-008-1 R2 and R3 have not been part of a FFT filing.

2. FAC-008-1 R2 and R3 are not subject to an on-going Standards Development Project.

3. FAC-008-1 R2 and R3 have a Lower VRF.

4. FAC-008-1 R2 and R3 are in the third tier of the AML.

5. The retirement of FAC-008-1 R2 and R3 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-008-1 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-1 R2 and R3, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These requirements may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-1 R2 and R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-1 R2 and R3.

FAC-008-3 R4; FAC-008-3 R5 – Facility Ratings

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.

Background/Commission Directives

FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[56] "On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No. 693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[57] FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[58]

There are no outstanding Commission directives that are affected by the proposed retirement of FAC-008-3 R4 and R5.

Technical Justification

[56] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[57] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[58] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).

FAC-008-3 R4 and R5 require that a Transmission Owner and Generator Owner must make its facilities ratings methodology available for inspection and technical review by Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated facilities are located and also require them to respond to any comments received including whether a change will be made to the facility ratings methodology. The retirement of FAC-008-3 R4 and R5 does not create a reliability gap, because Transmission Owners and Generator Owners must comply with the substantive requirements of FAC-008-3 regarding their facility rating methodologies whether or not the exchange envisioned by FAC-008-3 R4 and R5 occurs. Further, neither FAC-008-3 R4 nor R5 require that the Transmission Owner and Generator Owner change its methodology, rather FAC-008-3 R4 and R5 are designed as an exchange of comments that may be an avenue to advance commercial interests.

For example, if a Generator Owner's methodology provides for derating its GSU transformers below the nameplate in an effort to extend the life of its GSUs, that is a commercial decision it has made, and should not be subject to review by a Reliability Coordinator, Transmission Operator, Transmission Planner, and Planning Authority, some of which may have affiliated parts of their company that could benefit from the Generator Owner changing its methodology and operating its GSUs at nameplate. In contrast, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner shall equal the most limiting applicable equipment rating, and consider, for example, emergency and normal conditions, historical performance, nameplate ratings, etc. is not significantly or substantively advanced by FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments). Furthermore, the reliability objective that facility ratings produced by the methodologies of the Transmission Owner or Generator Owner are provided to the reliability entities for the establishment of SOLs, IROLs, calculations for MOD requirements and compliance with the TPL Standards is accomplished without FAC-008-3 R4 (available for inspection) and R5 (comment and responsive comments).[59] Accordingly, the requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-008-3. Instead of spending time and resources on FAC-008-3 R4 and R5, Generator Owners' and Transmission Owners' time and resources would be better spent complying with the substantive requirements of FAC-008-3. For these same reasons, the ERO compliance program would gain

[59] See MOD-001-1a R9, MOD-028-1 R2.3; MOD-029-1a R2.1; MOD-030-2 R3.1, PRC-023-2, Attachment A 2.7; TPL-001-0.1 Footnote a; TPL-002-1b, footnotes a and b; TPL-003-0a, footnote a and TPL-004-0, footnote a. Also, via FAC-011-2 the System Operating Limits methodology of Reliability Coordinator may also use facility ratings as a key element. Also, FAC-008-3 R7 and R8 require the transmission of facility ratings to reliability entities.

efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Transmission Owner's or Generator Owner's adherence to substantive requirements of FAC-008-3.

Criterion A

The requirements in FAC-008-3 R4 and R5 to make the facility ratings methodology available for comment (and if comments are received to respond to those comments) is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-008-3 R4 and R5 have not been part of a FFT filing.

2. FAC-008-3 R4 and R5 are not subject to an on-going Standards Development Project.

3. FAC-008-3 R4 and R5 have a Lower VRF.

4. FAC-008-3 R4 and R5 are in the third tier of the AML.

5. The retirement of FAC-008-3 R4 and R5 does not pose any negative impact to the following applicable NERC's published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-008-3 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. Retirement of FAC-008-3 R4 and R5, does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability. These may invite entities to engage in an exchange or debate over commercially sensitive information.

7. The retirement of FAC-008-3 R4 and R5 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-008-3 R4 and R5.

***FAC-010-2.1 R5 – System Operating Limits Methodology for the Planning Horizon*

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives

FAC-010-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[60] FAC-010-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[61] FAC-010-2.1 was filed for Commission approval on November 20, 2009 in Docket No. RD10-9-000 and was approved on April 19, 2010.[62] In Order No. 722,[63] the Commission approved FAC-010-2.1 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

Technical Justification

The reliability purpose of FAC-010-2.1, to ensure that System Operating Limits used in the reliable planning of the BES are determined based on an established methodology, is unaffected by the proposed retirement of R5. FAC-010-2.1 R5 requires that when a Planning Authority receives comments on its SOL methodology, it must respond and

[60] *Facilities Design, Connections and Maintenance Reliability Standards*, 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).
[61] *Version Two Facilities Design, Connections and Maintenance Reliability Standards*, 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).
[62] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Transmission Operations Reliability Standards, Docket No. RD10-9-000 (April 19, 2010).
[63] *Version Two Facilities Design, Connections and Maintenance Reliability Standards* 125 FERC ¶ 61,040 (2009).

indicate whether it has changed its methodology. The retirement of FAC-010-2.1 R5 does not create a reliability gap, because the Planning Authority must comply with the substantive requirements of FAC-010-2.1 whether or not the exchange envisioned by FAC-010-2.1 R5 occurs. FAC-010-2.1 R5 may support an avenue to advance commercial interests.

For example, if a Transmission Operator or Transmission Planner is also a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Planning Authority's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of its development of a facility ratings methodology under FAC-008-1, -3 than the Planning Authority's methodology. FAC-010-2.1 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Planning Authority's SOL methodology. Accordingly, FAC-010-2.1 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-010-2.1. Instead of spending time and resources on FAC-010-2.1, a Planning Authority's time and resources would be better spent complying with the substantive requirements of FAC-010-2.1. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Planning Authority's adherence to substantive requirements of FAC-010-2.1.

Criterion A
The requirement in FAC-010-2.1 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C
1. FAC-010-2.1 R5 has not been part of a FFT filing.

2. FAC-010-2.1 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011. Thus, it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-010-2.1 R5 has a Lower VRF.

4. FAC-010-2.1 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-010-2.1 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-010-2.1 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-010-2.1 R5.

***FAC-011-2 R5– System Operating Limits Methodology for the Operations Horizon*

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.

Background/Commission Directives

FAC-011-1 was filed for Commission approval on November 15, 2006 in Docket Nos. RM06-16-000 and RM07-3-000 and was approved on December 27, 2007 in Order No. 705.[64] FAC-011-2 was filed for Commission approval on June 30, 2008 in Docket No. RM08-11-000 and was approved on March 20, 2009 in Order No. 722.[65] In Order No. 722, the Commission approved FAC-011-2 R5 without specifically addressing R5.

There are no outstanding Commission directives with respect to this R5.

Technical Justification

FAC-011-2 R5 requires that when a Reliability Coordinator receives comments on its SOL methodology that it must respond and indicate whether it has changed its methodology. The retirement of FAC-011-2 R5 does not create a reliability gap, because the Reliability Coordinator must comply with the substantive requirements of FAC-011-2 R5 whether or not the exchange envisioned by FAC-011-2 R5 occurs. FAC-011-2 R5 may support an avenue to advance commercial interests.

For example, similar to FAC-010-2.1 R5, if a Transmission Operator or Transmission Planner also is a Transmission Owner it may have a commercial interest in lowering SOLs on its transmission lines in an effort to extend the life of its equipment and, therefore, challenge the Reliability Coordinator's methodology to reduce its SOLs. The Transmission Owner's interests are better considered in the context of the development of its facility ratings methodology under FAC-008-1, -3 than the Reliability Coordinator's methodology. FAC-011-2 R5, however, is an invitation to advance commercial interests not through established means, but by challenging the Reliability Coordinator's SOL methodology. Accordingly, FAC-011-2 R5 sets forth an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues. (Criteria A, B1, B4 and B6). In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-011-2. Instead of spending time and resources on FAC-011-2 R5 a Reliability Coordinator's time and resources would be better spent complying with the substantive requirements of FAC-011-2 R5. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-011-2 R5.

Criterion A

[64] *Facilities Design, Connections and Maintenance Reliability Standards*, 121 FERC ¶ 61,296 (December 27, 2007) (Order No. 705).

[65] *Version Two Facilities Design, Connections and Maintenance Reliability Standards*, 126 FERC ¶ 61,255 (March 20, 2009) (Order No. 722).

The requirement in FAC-011-2 R5 to respond to comments on the SOL methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-011-2 R5 has not been part of a FFT filing.

2. FAC-011-2 R5 is subject to future Standards Development Project 2012-11 FAC Review, which is a placeholder for the five year review of FAC-010 and FAC-011which is not currently scheduled and thus it is appropriate to process the retirement of this requirement as part of the P81 Project.

3. FAC-011-2 R5 has a Lower VRF.

4. FAC-011-2 R5 is not on the AML.

5. The retirement of this requirement does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-011-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of this requirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-011-2 R5 also promotes a results-based approach because the requirements have no direct nexus to the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-011-2 R5.

FAC-013-2 R3 – Assessment of Transfer Capability for the Near-term Transmission Planning Horizon

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.

Background/Commission Directives

FAC-013-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[66] FAC-013-2 was submitted for Commission approval on January 28, 2011 in Docket No. RD11-3-000 and was approved on November 17, 2011.[67]

In Order No. 729, the Commission denied NERC's request to withdraw FAC-012-1 and retire FAC-013-1, and directed as follows at paragraph 291:

> 291. The Commission hereby adopts its NOPR proposal to deny NERC's request to withdraw FAC-012-1 and retire FAC-013-1. Instead, pursuant to section 215(d)(5) of the FPA and section 39.5(f) of our regulations, the Commission directs the ERO to develop modifications to FAC-012-1 and FAC-013-1 to comply with the relevant directives of Order No. 693 and, as otherwise necessary, to make the requirements of those Reliability Standards consistent with those of the MOD Reliability Standards approved herein as well as this Final Rule. These modifications should also remove redundant provisions for the calculation of transfer capability addressed elsewhere in the MOD Reliability Standards. In making these revisions, the ERO should consider the development of a methodology for calculation of inter-regional and intra-regional transfer capabilities. The Commission accepts the ERO's request for additional time to prepare the modifications and so directs the ERO to submit the modifications to FAC-012-1 and FAC-013-1 no later than 60 days before the MOD Reliability Standards become effective.

[66] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[67] *Order Approving Reliability Standard*, 137 FERC ¶ 61,131 (2011).

Although the Commission did not directly address the merits of FAC-013-2 R3 when approving FAC-013-2,[68] similar to FAC-008-3, the developer of the Transfer Capability methodology and data must follow specific technical requirements and provide the data to reliability entities for use in their models. There are no outstanding Commission directives with respect to this R3.

Technical Justification

A review of FAC-013-2 R3 indicates that it is a needlessly burdensome administrative task that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B4). Specifically, FAC-013-2 R1 and its sub-requirements set forth the information that each Planning Authority must include when developing its Transfer Capability methodology. FAC-013-2 R3 sets forth a requirement that if an entity comments on this methodology, the Planning Authority must respond and indicate whether or not it will make a change to its Transfer Capability methodology. Thus, while R1 sets forth substantive requirements, R3 sets forth more of an administrative task of the Planning Authority responding to comments on its methodology.

The following NERC glossary definition of Transfer Capability states:

> The measure of the ability of interconnected electric systems to move or transfer power *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is *not g*enerally equal to the transfer capability from "Area B" to "Area A."

In the context of a Planning Authority engaging in an exchange with an entity over the Transfer Capability there is a possibility of a scenario that a group of generators[69] try to get the Planning Authority to revise its Transfer Capability methodology to advance commercial interests via changes to the methodology that would increase or decrease transfer capability from Area A to Area B. (Criterion B6). Such issues should be raised in the context of receipt of transmission services, not the Reliability Standards. Moreover, even without the possible commercial motivation of certain entities to get the Planning Authority to revise its Transfer Capability methodology, implementing an exchange between entities and the Planning Authority seems much better suited via regional planning committees, than mandatory Reliability Standards.

In this context, it would seem unnecessarily burdensome to engage in the exchange of comments, given there is no nexus between the exchange and compliance with the substantive requirements of FAC-013-2. Instead of spending time and resources on

[68] *Id.* (approval of FAC-013-2).

[69] Generators that receive the Transfer Capability methodology via an association with one of the entities in the R2 sub-requirements.

FAC-013-2 R3, time and resources would be better spent complying with the substantive requirements of FAC-013-2. For these same reasons, the ERO compliance program would gain efficiencies by no longer having to track whether requests for technical review had occurred, comments provided and reallocate time and resources to monitoring the Reliability Coordinator's adherence to substantive requirements of FAC-013-2.

Criterion A
The requirement in FAC-013-2 R3 to respond to comments on the Transfer Capability methodology is an administrative task that does little, if anything, to benefit or protect the reliable operation of the BES, and has the potential to implicate commercially sensitive issues.

Criteria B

- Criterion B1 (Administrative)
- Criterion B4 (Reporting)
- Criterion B6 (Commercial or Business Practice)

Criteria C

1. FAC-013-2 R3 has not been part of a FFT filing.

2. FAC-013-2 R3 is not subject to an on-going Standards Development Project.

3. FAC-013-2 R3 has a Lower VRF.

4. FAC-013-2 R3 is not on the AML.

5. The retirement of FAC-013-2 R3 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of FAC-013-2 that promotes these posted reliability principles, and not receiving comments on the facility ratings methodology from outside entities and then responding to those comments.

6. The retirement of FAC-013-2 R3 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of FAC-013-2 R3 promotes a results-based approach because the requirements do not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire FAC-013-2 R3.

INT-007-1 R1.2 – Interchange Confirmation

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

Background/Commission Directives
INT-007-1 was submitted for Commission approval on August 28, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[70] The Commission did not directly address INT-007-1 R1.2 when it approved the Reliability Standard in Order No. 693 at paragraph 867.

There are no outstanding Commission directives with respect to R1.2.

Technical Justification
The reliability purpose of INT-007-1 is to ensure that each Arranged Interchange is checked for reliability before it is implemented. The reliability purpose of INT-007-1 is unaffected by the proposed retirement of R1.2.

INT-007-1 R1.2 is a needlessly burdensome administrative task that does not support reliability because it is now outdated. (Criterion B1). At one time the identification number came from the NERC TSIN system, by now it is handled via NAESB Electric Industry Registry.[71] Also, under the E-Tag protocols, no entity may engage in an Interchange transaction without first registering with the E-Tag system and receiving an identification number. Further, the entity desiring the transaction enters this identification number in the E-Tag system to pre-qualify and engage in an Arranged Interchange. Accordingly, the task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES. (Criterion A). The ERO compliance program would benefit and be more efficient if it was not monitoring an outdated requirement.

[70] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[71] *See, North American Energy Standards Board Webregistry Technical Guide v1.4* (Proprietary) (July 2012). The new NAESB system has updated and implemented more automation to the process.

Criterion A
The task set forth in INT-007-1 R1.2 is an outdated activity that is no longer necessary, and thus, does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1 (Administrative)

Criteria C
1. INT-007-1 R1.2 has not been part of a FFT filing.

2. INT-007-1 R1.2 is part of a pending Standards Development Project – Project 2008-12 Coordinate Interchange Standards, which is estimated to start in the second quarter of 2013. Given this timeline, it is appropriate to move forward with the retirement of INT-007-1 R1.2. Such a retirement may also help to streamline Project 2008-12 once it is active and progressing.

3. INT-007-1 R1.2 has a Lower VRF.

4. INT-007-1 R1.2 is not on the AML.

5. The retirement of INT-007-1 R1.2 does not pose any negative impact to NERC's published and posted reliability principles No. 1 or No. 3.

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

   It is the adherence to the substantive requirements of INT-007-1 that promotes these posted reliability principles, not R1.2.

6. The retirement of INT-007-1 R1.2 does not impact any defense in depth strategies because the task is no longer necessary.

7. The retirement of INT-007-1 R1.2 promotes a results-based approach because the requirement does not require the performance of a reliability task.

Accordingly, for the above reasons, it is appropriate to retire INT-007-1 R1.2.

IRO-016-1 R2 – Coordination of Real-time Activities Between Reliability Coordinators

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

Background/Commission Directives
IRO-016-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693. The Commission did not directly address R2 when approving IRO-016-1 in Order No. 693 at paragraphs 1004 and 1005. There are no outstanding Commission directives with respect to R2.

Technical Justification
The reliability purpose of IRO-016-1 is to ensure that each Reliability Coordinator's operations are coordinated such that they will not have an adverse reliability impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations. To implement the purpose, IRO-016-1 R1 and its sub-requirements state:

> **R1.** The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
>
> **R1.1.** If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.
>
> **R1.2.** If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
>
> **R1.2.1.** If time permits, this re-evaluation shall be done before taking corrective actions.
>
> **R1.2.2.** If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

These requirements are specific actions and decision points among Reliability Coordinators that promote the reliable operation of the BES. In contrast, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Therefore, the reliability purpose of IRO-016-1 is unaffected by the proposed retirement of R2.

Furthermore, outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit data and information for purposes of monitoring compliance. Thus, the retirement of IRO-016-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to demonstrate compliance with IRO-016-1 R1 and its sub-requirements. Accordingly, retiring IRO-016-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. Thus, IRO-016-1 R~~1~~2 does not support reliability. Consequently, R2 is an administrative and data collection requirement ~~that~~ that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as IRO-016-1 R2 being a data, evidence and record retention requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401. In this regard, for the ERO, Regional Entities and the entities, arguably Reliability Standards are more difficult to understand because of this inconsistent approach (typically only implicitly requiring documentation as a part of an obligation to prove compliance, but occasionally explicitly requiring it with no discernible pattern or rationale).

Criterion A
A review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. IRO-016-1 R2 has not been part of a FFT filing

2. IRO-016-1 R2 is not subject to an on-going Standards Development project.

3. IRO-016-1 R2 has a Lower VRF.

4. IRO-016-1 R2 is not on the AML.

5. The retirement of IRO-016-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, since none of the principles appear to apply to a data retention requirement.

6. IRO-016-1 R2 does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of IRO-016-1 R2 promotes a results-based approach because the requirement is administrative and data collection, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire IRO-016-1 R2.

NUC-001-2 R9.1; NUC-001-2 R9.1.1; NUC-001-2 R9.1.2; NUC-001-2 R9.1.3; NUC-001-2 R9.1.4 – Nuclear Plant Interface Coordination

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement.

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3. A requirement to review the agreement(s) at least every three years.

R9.1.4. A dispute resolution mechanism.

Background/Commission Directives

NUC-001-1 was submitted for Commission approval on November 19, 2007 in Docket No. RM08-3-000 and was approved on October 16, 2008.[72] NUC-001-2 was submitted for Commission approval on August 14, 2009 in Docket No. RD09-10-000 and was approved on January 21, 2010.[73]

Although in Order No. 716 the merits of R9.1 and its sub-requirements were not directly addressed, the Commission did state the following in the context of the VRFs for all of R9:[74]

[72] *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008) ("Order No. 716"), *order on reh'g*, Order No. 716-A, 126 FERC ¶ 61,122 (2009).

[73] *Order Approving Reliability Standard*, 130 FERC ¶ 61,051 (2010).

[74] NUC-001-1 was approved in Order No. 716, while NUC-001-2 was approved without discussion of R9.1 and its sub-requirements in a subsequent order. *Mandatory Reliability Standard for Nuclear Plant Interface Coordination*, 125 FERC ¶ 61,065 (2008); 130 FERC ¶ 61,051 (2010).

> Consistent with the NOPR, the Commission directs the ERO to revise the violation risk factor assignment for Requirement R9 from lower to medium. The Commission disagrees with commenters that a lower violation risk factor is appropriate because Requirement R9 is an administrative requirement to include the specified provisions. While the Commission recognized in the NOPR that many of the requirements of the proposed Reliability Standard are administrative in nature, these same requirements provide for the development of procedures to ensure the safe and reliable operation of the grid, and responses to potential emergency conditions.

There are no outstanding Commission directives with respect to these requirements.

Technical Justification

The reliability purpose of NUC-001-2 is to ensure the coordination between Nuclear Plant Generator Operators and Transmission Entities for nuclear plant safe operation and shutdown. The reliability purpose of NUC-001-2 is unaffected by the proposed retirement of requirements 9.1, 9.1.1, 9.1.2, 9.1.3 and 9.1.4. Requirement 9.1 and its sub-requirements specify certain administrative elements that must be included in the agreement (required by R2) between the Nuclear Plant Generator Operator and the applicable Transmission Entities. These are a mix of technical, communication, training and administrative requirements. Of those that may be classified as administrative, R9.1 and its sub-requirements clearly stand out as unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A and B1). R9.1 and its sub-requirements are a check list of certain non-technical boilerplate provisions generally included in modern agreements. These provisions do not directly relate to protecting BES reliability. Further, requiring via a mandatory Reliability Standard the inclusion of boilerplate provisions is ~~an~~ unnecessarily burdensome relative to the other significant requirements in NUC-001-2 that pertain to performance based reliability coordination and protocols between Transmission Entities and Nuclear Plant Generator Operators. Therefore, the retirement of NUC-001-2 R9.1 and all its sub-requirements creates no reliability gap and are the type of provisions that would likely be in a modern agreement anyway.

For these same reasons, the ERO compliance program efficiency will increase with the retirement of NUC-001-2 R9.1 and its sub-requirements because compliance monitoring time and resources will not be spent conducting a checklist of whether an agreement includes boilerplate provisions, and instead, the time and resources may be spent reviewing adherence with the technical, substantive coordination and protocol provisions of NUC-001-2.

Criterion A

R9.1 and its sub-requirements are unnecessarily burdensome administrative tasks that do little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1 (Administrative)

Criteria C

1. NUC-001-2 R9.1 and its sub-requirements have not been part of a FFT filing.

2. NUC-001-2 R9.1 and its sub-requirements are not part of an on-going Standards Development Project, but NUC-001-2 is part of Project 2012-13, which is a placeholder for a five year review. Given the as yet undetermined start date for Project 2012-13, it is appropriate to move forward with the retirement of NUC-001-2 R9.1 and its sub-requirements.

3. Individual VRFs are not assigned to the sub-requirements of NUC-001-2 R9.

4. NUC-001-2 R9.1 and its sub-requirements are in the third tier of the AML.

5. The retirement of NUC-001-2 R9.1 and its sub-requirements do not pose any negative impact to NERC's published and posted reliability principles, since none of them seem to apply to the inclusion of boilerplate contractual provisions.

6. There is no impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of NUC-001-2 R9.1 and its sub-requirements promote a results-based approach by eliminating administrative check-list requirements.

Accordingly, for the above reasons, it is appropriate to retire NUC-001-2 R9.1 and its sub-requirements.

PRC-010-0 R2 – Assessment of the Design and Effectiveness of UVLS Program;

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).

Background/Commission Directives

PRC-010-0 was filed for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[75] Although not

[75] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

specifically addressing PRC-010-0 R2, in Order No. 693 at paragraph 1506 and 1507 the Commission stated that:

> With regard to ISO-NE's disagreement on integration of various system protections "because such integration cannot be technologically accomplished", we note that the evidence collected in the Blackout Report indicates that "the relay protection settings for the transmission lines, generators and underfrequency load shedding in the northeast may not be entirely appropriate and are certainly not coordinated and integrated to reduce the likelihood and consequence of a cascade – nor were they intended to do so." In addition, the Blackout Report stated that one of the common causes of major outages in North America is a lack of coordination on system protection. The Commission agrees with the protection experts who participated in the investigation, formulated Blackout Recommendation No. 21 and recommended that UVLS programs have an integrated approach.
>
> Regarding FirstEnergy's question of whether universal coordination among UVLS programs that address local system problems makes sense, we believe that PRC-010-0's objective in requiring an integrated and coordinated approach is to address the possible adverse interactions of these protection systems among themselves and to determine whether they could aggravate or accelerate cascading events. We do not believe this Reliability Standard is aimed at universal coordination among UVLS programs that address local system problems. (Footnote omitted).

The retirement of PRC-010-0 R2 does not affect a Commission directive.

Technical Justification

Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its current UVLS program assessment for purposes of monitoring compliance. Thus, the retirement of PRC-010-0 R2 does not affect the ability of NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-010-0 R1 and its sub-requirements. Furthermore, PRC-010-0 R1 requires that the entity document an assessment of the effectiveness of its UVLS program:

> The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program.

Accordingly, retiring PRC-010-0 R2 presents no gap to reliability or to the information NERC and the Regional Entity need to monitor compliance. A review of R2 indicates that it is a needlessly burdensome administrative and data collection/retention requirement that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, there are some inherent inefficiencies that result by a small number of requirements, such as PRC-010-0 R2 being a data production requirement, while there are other and more appropriate established methods to collect and review the data than a Reliability Standard via Rules of Procedure Section 401.

Criterion A
R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B
- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C
1. PRC-010-0 R2 has not been part of a FFT filing.

2. PRC-010-0 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-010-0 R2 in the P81 Project.

3. This requirement has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-010-0 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact on a defense in depth strategy because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-010-0 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-010-0 R2.

PRC-022-1 R2 – Under-Voltage Load Shedding Program Performance

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.

Background/Commission Directives
PRC-022-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[76] In Order No. 693 at paragraph 1565 the Commission approved PRC-022-1 without a discussion of R2. There are no outstanding Commission directives with respect to R2.

Technical Justification
Outside the context of a Reliability Standard, under Section 400 of the NERC Rules of Procedure, NERC and the Regional Entities have the authority to require an entity to submit documentation of its analysis of UVLS program performance for purposes of monitoring compliance. Thus, the retirement of PRC-022-1 R2 does not affect the ability for NERC and the Regional Entities to require Reliability Coordinators to produce documentation to monitor compliance with PRC-022-1 R1 and its sub-requirements. Furthermore, PRC-022-1 R1 already requires that the entity document UVLS performance:

> Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations.

Accordingly, retiring PRC-022-1 R2 presents no gap to reliability or to the information NERC and the Regional Entities need to monitor compliance. In this context, a review of R2 indicates that it is a needlessly burdensome administrative and data collection requirement that that does little, if anything, to benefit or protect the reliable operation of the BES. (Criteria A, B1 and B2). Also, similar to the retention of records requirements in CIP-007-3, -4 R7.3, FAC-002-1 R2 and PRC-010-0 R2, the ERO compliance program efficiency will increase since it will no longer need to track a static requirement of whether a UVLS program assessment was submitted within 30 days of a request by NERC or the Regional Entity, and instead, compliance monitoring may focus on the more substantive requirements of PRC-022-1.

Criterion A

[76] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

R2 is an administrative and data collection requirement that does little, if anything, to benefit or protect the reliable operation of the BES.

Criteria B

- Criterion B1(Administrative)
- Criterion B2 (Data Collection/Data Retention)

Criteria C

1. PRC-022-1 R2 has not been part of a FFT filing.

2. PRC-022-1 R2 is subject to Standards Development Project 2008-02 Undervoltage Load Shedding, which is not currently active and is only estimated to be completed until the second quarter of 2014. Since the purpose of Project 2008-02 does not necessarily include a review of R2 and its 2014 completion date is well into the future, it is appropriate to include PRC-022-1 R2 in the P81 Project.

3. PRC-022-1 R2 has a Lower VRF.

4. This requirement is not part of the AML.

5. The retirement of PRC-022-1 R2 does not pose any negative impact to NERC's published and posted reliability principles, particularly since submission of a program assessment or documentation of its analysis of UVLS program performance to a Regional Entity does not seem to implicate any of the principles.

6. For similar reasons, there is no negative impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of PRC-022-1 R2 promotes a results-based approach because it is a data collection requirement, and, therefore, does not provide the foundation for performing a reliability task.

Accordingly, for the above reasons, it is appropriate to retire PRC-022-1 R2.

***VAR-001-2 R5 – Voltage and Reactive Control*

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

Background/Commission Directives
VAR-001-1 was submitted for Commission approval on April 4, 2006, in Docket No. RM06-16-000. When approving VAR-001-1, in Order No. 693 at paragraph 1858,[77] the Commission recognized:

> . . . that all transmission customers of public utilities are required to purchase Ancillary Service No. 2 under the OATT or self-supply, but the OATT does not require them to provide information to transmission operators needed to accurately study reactive power needs. The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities.

On September 9, 2010, NERC submitted VAR-001-2, which included revisions to Requirement R5 to satisfy Commission directives in Order No. 693, including the directive in paragraph 1858. This directive was addressed by adding "Load Serving Entities" to the standard as applicable entities and making them subject to the same requirements as Purchasing Selling Entities. These modifications to VAR-001-2 were accepted by the Commission on January 10, 2011.[78]

Technical Justification
VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* open access transmission tariff ("OATT"). (Criteria A and B7). To elaborate, VAR-001-2 R5 provides for the PSE and LSE (transmission customers) to arrange for or self provide reactive resources the same as required under Schedule 2 of the OATT. Specifically, as a general matter Schedule 2 of the OATT states:

> **Schedule 2 Reactive Supply and Voltage Control from Generation or Other**
>
> In order to maintain transmission voltages on the Transmission Provider's transmission facilities within acceptable limits, generation facilities and non-generation resources capable of providing this service that are under the control of the control area operator) are operated to produce (or absorb) reactive power. Thus, Reactive Supply and Voltage Control from Generation or Other Sources Service must be provided for each transaction on the Transmission Provider's transmission facilities. The amount of Reactive Supply and Voltage Control from Generation or Other Sources Service that must be supplied with respect to the Transmission Customer's transaction will be determined based on the reactive power support necessary to maintain transmission voltages within limits that are

[77] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[78] *North American Electric Reliability Corp.*, 134 FERC ¶ 61,015 (2011).

> generally accepted in the region and consistently adhered to by the Transmission Provider.
>
> Reactive Supply and Voltage Control from Generation or Other Sources Service is to be provided directly by the Transmission Provider (if the Transmission Provider is the Control Area operator) or indirectly by the Transmission Provider making arrangements with the Control Area operator that performs this service for the Transmission Provider's Transmission System. The Transmission Customer must purchase this service from the Transmission Provider or the Control Area operator. A Transmission Customer may satisfy all or part of its obligation through self provision or purchases provided that the self-provided or purchased reactive power reduces the Transmission Provider's reactive power requirements and is from generating facilities under the control of the Transmission Provider or Control Area operator. The Transmission Customer's Service Agreement shall specify any such reactive supply arrangements. To the extent the Control Area operator performs this service for the Transmission Provider, charges to the Transmission Customer are to reflect only a pass-through of the costs charged to the Transmission Provider by the Control Area operator. The Transmission Provider's rates for Reactive Supply and Voltage Control from Generation Sources Services shall be set out in Appendix A to this Schedule.

Given the importance of the procurement or self providing of reactive power, even in a market setting a form of Schedule 2 is found in the tariffs of MISO and PJM, for example. Also, other contractual mechanism, such as Interchange agreements, also are used to ensure transmission customers (suc as PSEs and LSEs) provide reactive power, While NERC complied with the Commission's directive to add LSEs to VAR-001-2 R5, a review of this requirement in light of Schedule 2 indicates that the reliability objective of ensuring that PSEs as well as LSEs either acquire or self provide reactive power resources associated with its transmission service requests is accomplished via Schedule 2, and, therefore, there is no need to reiterate it in VAR-001-2 R5. The repetitive nature of VAR-001-2 R5 is also apparent in the context of how a PSE or LSE generally demonstrates compliance – via screenshots from Open Access Same-Time Information System ("OASIS") reservations that show the mandatory acquiring or self providing of reactive power resources per Schedule 2.

The reliability objective of VAR-001-2 is also accomplished in VAR-001-2 R2 (that is not proposed for retirement) which reads:

> Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, [sic] and controllable load – within its area to protect the voltage levels under normal and

Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

The Transmission Operator's adherence to R2 is a double check for the obligations under Schedule 2 to ensure there are sufficient reactive power resources to protect the voltage levels under normal and Contingency conditions. This double check, however, does not relieve PESs and LESs from their obligations under Schedule 2 of the OATT or Interchange agreements.

In addition, in the Electric Reliability Council of Texas (ERCOT) region, where there is no FERC approved OATT, reactive power is handled via Section 3.15 of the ERCOT Nodal Protocols that describes how ERCOT establishes a Voltage Profile for the grid, and then in detail explains the responsibilities of the Generators, Distribution Providers and Texas Transmission Service Providers (not to be confused with a NERC TSP), to meet the Voltage Profile and ensure that those entities have sufficient reactive support to do so. There is further Operating Guide detail on the responsibilities for entities to deploy reactive resources approximately, within performance criteria in the Operating Guide Section 3. Thus, as in non-ERCOT regions, ERCOT has protocols that are duplicative of VAR-001-2 R5.

Given the redundant nature of VAR-001-2 R5 it would also assist the ERO compliance program to retire it, so that time and resources can be reallocated to focus on adherence to other Reliability Standard requirements.

Criterion A
VAR-001-2 R5 does little, if anything, to benefit or protect the reliable operation of the BES because it is redundant with FERC's *pro forma* OATT.

Criteria B

- Criterion B7 (Redundant)

Criteria C

1. VAR-001-2 R5 has not been part of a FFT filing.

2. VAR-001-2 R5 is subject to Standards Development Project 2008-01 Voltage and Reactive Planning Control. Given that Project 2008-01 is not currently active and is only estimated to be completed until the second quarter of 2014 and the purpose of this project does not necessarily include a review of R5, it is appropriate to include VAR-001-2 R5 in the P81 Project. Also, retiring this requirement via P81 Project may facilitate the efficiency of Project 2008-01.

3. This requirement has a High VRF. However, the reliability objective of VAR-001-2 R5 will be accomplished via Schedule 2 of the OATT, ERCOT protocols and R2 of VAR-001-2. Thus, the High VRF is not dispositive, and VAR-001-2 R5 remains appropriate for retirement.

4. VAR-001-2 R5 is in the third tier of the AML.

5. Because VAR-001-2 R5 is redundant with the *pro forma* OATT and ERCOT protocols, (as well as the reliability objective of VAR-001-2 R5 is accomplished via Schedule 2 of the OATT, ERCOT protocols and R2 of VAR-001-2), the retirement of VAR-001-2 R5 does not pose any negative impact to the following NERC published and posted reliability principles:

   Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

   Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

6. Retirement does not negatively impact defense in depth because no other requirement depends on it to help cover a reliability gap or risk to reliability.

7. The retirement of VAR-001-2 R5 is neutral regarding whether it promotes a results-based approach because the requirement is results-based, but already covered in the *pro forma* OATT, Schedule 2 and ERCOT protocols.

Accordingly, for the above reasons, it is appropriate to retire VAR-001-2 R5.

V. The Initial Phase Reliability Standards Provided for Informational Purposes

The following requirements are already scheduled to be retired or subsumed via another Standards Development Project that has been approved by stakeholders and the NERC Board of Trustees (or due to be before the NERC Board of Trustees in November), and, thus, are presented here for informational purposes only. For regulatory efficiency, these requirements will not be presented for comment and vote, and, therefore, will not be presented to the NERC Board of Trustees for approval or filed with the Commission or Canadian governmental authorities as part of the P81 Project.

CIP-001-2a R4 Sabotage Reporting

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

Background

CIP-001-1 was filed for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[79] CIP-001-1a was filed for Commission approval on April 21, 2010 in Docket No. RD10-11-000, and was approved by an unpublished letter order on February 2, 2011.[80]

CIP-001-2a was filed for Commission approval as a Regional Variance for the ERCOT Region, containing an interpretation of CIP-001-1, on June 21, 2011 in Docket No. RD11-6-000 and was approved by unpublished letter order on August 2, 2011.[81]

As part of EOP-004-2, on November 5, 2012, stakeholders approved the retirement of CIP-001-2a R4. EOP-004-2 was approved by the NERC Board of Trustees on November 7, 2012. Thus, CIP-001-2a R4 is presented here for informational purposes only.

COM-001-1.1 R6- Telecommunications

Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."

Background

COM-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[82] COM-001-1.1 was submitted for Commission approval on February 6, 2009 in Docket No. RD09-2-000 as errata and was approved by unpublished letter order on May 13, 2009.[83]

---

[79] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[80] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of Interpretation to Reliability Standard CIP-001-1 —Cyber Security— Sabotage Reporting, Requirement R2, Docket No. RD10-11-000 (February 2, 2011).

[81] Letter Order, Petition of the North American Electric Reliability Corporation for Approval of the Reliability Standard CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity, Docket No. RD11-6-000 (August 2, 2011).

[82] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[83] Letter Order, Electric Reliability Organization Errata Petition Updating Accepted Reliability Coordination and Transmission Operations Reliability Standards, Docket No. RD09-2-000 (May 13, 2009).

As part of COM-001-2, on September 17, 2012, stakeholders approved the retirement of COM-001-1.1 R6 in Project 2006-06 (Reliability Coordination). This project is due to be presented to the NERC Board of Trustees in November. Thus, COM-001-1 R6 is presented here for informational purposes only.

EOP-004-1 R1 – Disturbance Reporting

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

Background

EOP-004-1 was submitted to the Commission for approval on November 15, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[84]

As part of EOP-004-2, on November 5, 2012, stakeholders approved the retirement of EOP-001-1 R1. EOP-004-2 was approved by the NERC Board of Trustees on November 7, 2012. Thus, EOP-001-1 R1 is presented here for informational purposes only.

EOP-009-0 R2 – Documentation of Blackstart Generating Unit Test Results

R2. The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

Background

EOP-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[85] In Order No. 749, the Commission approved the retirement of EOP-009-0 as of July 1, 2013, based on the approval of EOP-005-2, which did not carry forward R2 of EOP-009-0. Thus, EOP-009-0 R2 is presented here for informational purposes only.

FAC-008-1 R1.3.5 – Facility Ratings Methodology

R1.3.5. Other assumptions.

Background

[84] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[85] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

FAC-008-1 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[86]

"On May 12, 2010, the NERC Board of Trustees approved the proposed FAC-008-2 Reliability Standard that addressed the first two of the FERC directives in Order No. 693. NERC's proposed FAC-008-2 Reliability Standard was not filed with FERC for approval, but instead was revisited by the standard drafting team so that the third Order No. 693 directive could be addressed in response to FERC's March 18, 2010 Order…"[87]

FAC-008-3 was submitted for Commission approval on June 15, 2011 in Docket No. RD11-10-000 and was approved on November 17, 2011.[88]

FAC-008-3 (which combined FAC-008 and FAC-009) has been approved by the Commission without the "other assumptions" language.[89] Since FAC-008-3 will become effective on January 1, 2013, FAC-008-1 R1.3.5 is presented here for informational purposes only.

PRC-008-0 R1; PRC-008-0 R2 – Underfrequency Load Shedding Equipment Maintenance Programs

R1. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.

R2. The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).

Background

[86] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[87] Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard FAC-008-3 — Facility Ratings, Docket No. RD11-10-000, (June 15, 2011).
[88] *Order Approving Reliability Standard*, 137 FERC ¶ 61,123 (2011).
[89] *Id.*

PRC-008-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[90]

Under Standards Development Project 2007-17 Protection System Maintenance, which recently passed on August 27, 2012, PRC-008-0 is scheduled to be retired, subsumed and replaced with PRC-005-2. PRC-005-2 will likely be presented to the NERC Board of Trustees in November for approval, and, thus, PRC-008-0 is only presented here for informational purposes.

PRC-009-0 R1; PRC-009-0 R1.1; PRC-009-0 R1.2; PRC-009-0 R1.3; PRC-009-0 R1.4; PRC-009-0 R2 – UFLS Performance Following an Underfrequency Event

R1. The Transmission Owner, Transmission Operator, Load-Serving Entity and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UFLS set points and tripping times.

R1.3. A simulation of the event.

R1.4. A summary of the findings.

R2. The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.

Background

PRC-009-0 was submitted for Commission approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.[91] In Order No.

[90] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[91] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

763 at paragraph 103[92] the Commission accepted the retirement of PRC-009-0 as appropriately replaced with PRC-006-1. Consistent with Order No. 763, PRC-009-0 will become inactive on September 30, 2013 and will be replaced by PRC-006-1. Thus, PRC-009-0 is presented here for informational purposes only.

TOP-001-1a R3 – Reliability Responsibilities and Authorities

R3. Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.

Background

TOP-001-1 was submitted for Commission approval on November 15, 2006 in Docket No. RM06-16-000 and was approved by the Commission on March 16, 2007 in Order No. 693.[93] TOP-001-1a was submitted for approval on July 16, 2010 in Docket No. RM10-29-000 and was approved on September 15, 2011 in Order No. 753.[94]

IRO-001-1a R8 reads:

> Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.

[92] *Automatic Underfrequency Load Shedding and Load Shedding Plans Re-liability Standards*, 139 FERC ¶ 61,098 (2012).
[93] *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007). ("Order No. 693"), *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).
[94] *Electric Reliability Organization Interpretation of Transmission Operations Reliability Standard*, 136 FERC ¶ 61,176, (September 15, 2011) (Order No. 753).

Although there is redundancy between TOP-001-1a R3 and IRO-001-1a R8 as related to Reliability Coordinators, this redundancy was addressed in Standards Development Project 2007-03 (Real-time Operations). Specifically, Project 2007-03 eliminated the redundancy in the current version of TOP-001-2 R1 that replaces TOP-001-1a R3 and reads:

> Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued and identified as such by its Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.

TOP-001-2 has been approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-001-1a R3 is presented for informational purposes only.

TOP-005-2a R1 – Operational Reliability Information

R1. As a condition of receiving data from the Interregional Security Network (ISN), each ISN data recipient shall sign the NERC Confidentiality Agreement for "Electric System Reliability Data."

Background

Without directly addressing R1 of TOP-005-1 or TOP-005-2a the Commission approved both versions of TOP-005.[95] A review of the Standards Development Project 2007-03 Real-time Transmission Operations indicates it proposes R1 of TOP-005-1 to be retired. The reasoning provided by the SDT was the following:

> Confidentiality is not a reliability issue, but a market or business issue. Since this is not a reliability issue, it does not belong in the Reliability Standards and can be deleted.[96]

As stated above, in the context of Project 2007-03, TOP-001-1a was approved by the NERC Board of Trustees and will be filed with the Commission for approval; therefore, TOP-005-2a R1 is presented for informational purposes only.

[95] Order No. 693 at paragraphs 1648 through 1652 (approval of TOP-005-1); *Mandatory Reliability Standards for Interconnection Reliability Operating Limits*, 134 F.E.R.C. ¶ 61,213 (2011) (approval of TOP-005-2a).

[96] Mapping Document Project 2007-03 Real-time Operations at page 31 (April 27 2012).

Appendix A

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
BAL-005-0.2b	**R2**	√							√			H		No	No	Yes
~~**CIP-001-2a**~~	~~**R4**~~	~~√~~	~~√~~	~~√~~	~~√~~					~~√~~	~~√~~	~~**M**~~	~~**2**~~	~~**No**~~	~~**No**~~	~~**Yes**~~
CIP-003-3, -4	**R1.2**	√	√							√	√	L	2	No	No	Yes
CIP-003-3, -4	**R3, R3.1 R3.2 R3.3**	√	√		√					√	√	L	3	No	No	Yes
CIP-003-3, -4	**R4.2**	√	√		√				√	√	√	L	3	No	No	Yes
CIP-005-3a, -4a	**R2.6**	√	√		√					√	√	L	1	No	No	Yes
CIP-007-3, -4	**R7.3**	√	√	√							√	L	1	No	No	Yes
~~**EOP-004-1**~~	~~**R1**~~	~~√~~	~~√~~		~~√~~						~~√~~	~~**L**~~	~~**3**~~	~~**No**~~	~~**No**~~	~~**Yes**~~
EOP-005-2	**R3.1**	√	√				√		√			N/A	2	No	No	Yes
FAC-002-1	**R2**	√	√	√								L	3	No	No	Yes
FAC-008-1	**R2, R3**	√	√			√		√				L	3	No	No	Yes
FAC-008-3	**R4**	√	√			√		√				L	3	No	No	Yes

December 20, ~~October 23,~~ 2012

			Criteria B							Criteria C						
Standard	**Req.**	**Criterion A**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
		Reliability Impact	Administrative	Data	Documentation	Reporting	Updates	Commercial	Redundant	FFT	Ongoing Project	VRF	AML Tier	Reliability Principles Implicated?	In-depth Protection Implicated?	Results-based promoted?
	R5															
FAC-010-2.1	**R5****	√	√			√		√				L		No	No	Yes
FAC-011-2	**R5****	√	√			√		√				L		No	No	Yes
FAC-013-2	**R3**	√	√			√		√				L		No	No	Yes
INT-007-1	**R1.2**	√	√									L		No	No	Yes
IRO-016-1	**R2**	√	√	√								L		No	No	Yes
NUC-001-2	**R9.1** **R9.1.1** **R9.1.2** **R9.1.3** **R9.1.4**	√	√									N/A	3	No	No	Yes
PRC-010-0	**R2**	√	√	√								L		No	No	Yes
PRC-022-1	**R2**	√	√	√								L		No	No	Yes
VAR-001-2	**R5****	√							√			H	3	No	No	Yes

Complete Violation Severity Levels Matrix

Encompassing All Commission-Approved Reliability Standards

September 21, 2012

Change History Table is located at the end of the document

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-001-0.1a	R1.	Each Balancing Authority shall operate such that, on a rolling 12-month basis, the average of the clock-minute averages of the Balancing Authority's Area Control Error (ACE) divided by 10B (B is the clock-minute average of the Balancing Authority Area's Frequency Bias) times the corresponding clock-minute averages of the Interconnection's Frequency Error is less than a specific limit. This limit is a constant derived from a targeted frequency bound (separately calculated for each Interconnection) that is reviewed and set as necessary by the NERC Operating Committee. ***See Standard for Formula.***	The Balancing Authority Area's value of CPS1 is less than 100% but greater than or equal to 95%.	The Balancing Authority Area's value of CPS1 is less than 95% but greater than or equal to 90%.	The Balancing Authority Area's value of CPS1 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS1 is less than 85%.
BAL-001-0.1a	R2.	Each Balancing Authority shall operate such that its average ACE for at least 90% of clock-ten-minute periods (6 non-overlapping periods per hour) during a calendar month is within a specific limit, referred to as L_{10}. ***See Standard for Formula.***	The Balancing Authority Area's value of CPS2 is less than 90% but greater than or equal to 85%.	The Balancing Authority Area's value of CPS2 is less than 85% but greater than or equal to 80%.	The Balancing Authority Area's value of CPS2 is less than 80% but greater than or equal to 75%.	The Balancing Authority Area's value of CPS2 is less than 75%.
BAL-001-0.1a	R3.	Each Balancing Authority providing Overlap Regulation Service shall evaluate Requirement R1 (i.e., Control Performance Standard 1 or CPS1) and Requirement R2 (i.e., Control Performance Standard 2 or CPS2) using the characteristics of the combined ACE and combined Frequency Bias Settings.	N/A	N/A	N/A	The Balancing Authority providing Overlap Regulation Service failed to use a combined ACE and frequency bias.
BAL-001-0.1a	R4.	Any Balancing Authority receiving Overlap Regulation Service shall not	N/A	N/A	N/A	The Balancing Authority receiving

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		have its control performance evaluated (i.e. from a control performance perspective, the Balancing Authority has shifted all control requirements to the Balancing Authority providing Overlap Regulation Service).				Overlap Regulation Service failed to ensure that control performance was being evaluated in a manner consistent with the calculation methodology as described in BAL-001-01 R3.
BAL-002-1	R1.	Each Balancing Authority shall have access to and/or operate Contingency Reserve to respond to Disturbances. Contingency Reserve may be supplied from generation, controllable load resources, or coordinated adjustments to Interchange Schedules.	N/A	N/A	N/A	The Balancing Authority does not have access to and/or operate Contingency Reserve to respond to Disturbances.
BAL-002-1	R1.1.	A Balancing Authority may elect to fulfill its Contingency Reserve obligations by participating as a member of a Reserve Sharing Group. In such cases, the Reserve Sharing Group shall have the same responsibilities and obligations as each Balancing Authority with respect to monitoring and meeting the requirements of Standard BAL-002.	N/A	N/A	N/A	The Balancing Authority has elected to fulfill its Contingency Reserve obligations by participating as a member of a Reserve Sharing Group and the Reserve Sharing Group has not provided the same responsibilities and obligations as required of the responsible entity with respect to monitoring and meeting the requirements of Standard BAL-002.
BAL-002-1	R2.	Each Regional Reliability Organization, sub-Regional Reliability	The Regional Reliability	The Regional Reliability	The Regional Reliability	The Regional Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Organization or Reserve Sharing Group shall specify its Contingency Reserve policies, including:	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 1 of the following sub-requirements.	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 2 or 3 of the following sub-requirements.	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify 4 or 5 of the following sub-requirements.	Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify all 6 of the following sub-requirements.
BAL-002-1	R2.1.	The minimum reserve requirement for the group.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the minimum reserve requirement for the group.
BAL-002-1	R2.2.	Its allocation among members.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the allocation of reserves among members.
BAL-002-1	R2.3.	The permissible mix of Operating Reserve – Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the permissible mix of Operating Reserve –

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Spinning and Operating Reserve – Supplemental that may be included in Contingency Reserve.
BAL-002-1	R2.4.	The procedure for applying Contingency Reserve in practice.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to provide the procedure for applying Contingency Reserve in practice.
BAL-002-1	R2.5.	The limitations, if any, upon the amount of interruptible load that may be included.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has failed to specify the limitations, if any, upon the amount of interruptible load that may be included.
BAL-002-1	R2.6.	The same portion of resource capacity (e.g. reserves from jointly owned generation) shall not be counted more than once as Contingency Reserve by multiple Balancing Authorities.	N/A	N/A	N/A	The Regional Reliability Organization, sub-Regional Reliability Organization, or Reserve Sharing Group has allowed the same portion of resource capacity (e.g., reserves from jointly owned generation) to be

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						counted more than once as Contingency Reserve by multiple Balancing Authorities.
BAL-002-1	R3.	Each Balancing Authority or Reserve Sharing Group shall activate sufficient Contingency Reserve to comply with the DCS.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 100% but greater than or equal to 95%.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 95% but greater than or equal to 90%.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 90% but greater than or equal to 85%.	The Balancing Authority or Reserve Sharing Group's Average Percent Recovery per the NERC DCS quarterly report was less than 85%.
BAL-002-1	R3.1.	As a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency. All Balancing Authorities and Reserve Sharing Groups shall review, no less frequently than annually, their probable contingencies to determine their prospective most severe single contingencies.	The Balancing Authority or Reserve Sharing Group failed to review their probable contingencies to determine their prospective most severe single contingencies annually.	N/A	N/A	The Balancing Authority or Reserve Sharing Group failed to carry at least enough Contingency Reserve to cover the most severe single contingency.
BAL-002-1	R4.	A Balancing Authority or Reserve Sharing Group shall meet the Disturbance Recovery Criterion within the Disturbance Recovery Period for 100% of Reportable Disturbances. The Disturbance Recovery Criterion is:	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 90% and less than 100% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Balancing Authority or Reserve Sharing Group met the Disturbance Recovery Criterion within the Disturbance Recovery Period for more than 0% and less than or equal to 70% of Reportable Disturbances.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-002-1	R4.1.	A Balancing Authority shall return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to zero. For negative initial ACE values just prior to the Disturbance, the Balancing Authority shall return ACE to its pre-Disturbance value.	N/A	N/A	N/A	The Balancing Authority failed to return its ACE to zero if its ACE just prior to the Reportable Disturbance was positive or equal to zero or for negative initial ACE values failed to return ACE to its pre-Disturbance value.
BAL-002-1	R4.2.	The default Disturbance Recovery Period is 15 minutes after the start of a Reportable Disturbance.	N/A	N/A	N/A	N/A
BAL-002-1	R5.	Each Reserve Sharing Group shall comply with the DCS. A Reserve Sharing Group shall be considered in a Reportable Disturbance condition whenever a group member has experienced a Reportable Disturbance and calls for the activation of Contingency Reserves from one or more other group members. (If a group member has experienced a Reportable Disturbance but does not call for reserve activation from other members of the Reserve Sharing Group, then that member shall report as a single Balancing Authority.) Compliance may be demonstrated by either of the following two methods:	The Reserve Sharing Group met the DCS requirement for more than 90% and less than 100% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 80% and less than or equal to 90% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 70% and less than or equal to 80% of Reportable Disturbances.	The Reserve Sharing Group met the DCS requirements for more than 0% and less than or equal to 70% of Reportable Disturbances.
BAL-002-1	R5.1.	The Reserve Sharing Group reviews group ACE (or equivalent) and demonstrates compliance to the DCS. To be in compliance, the group ACE (or its equivalent) must meet the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.				
BAL-002-1	R5.2.	The Reserve Sharing Group reviews each member's ACE in response to the activation of reserves. To be in compliance, a member's ACE (or its equivalent) must meet the Disturbance Recovery Criterion after the schedule change(s) related to reserve sharing have been fully implemented, and within the Disturbance Recovery Period.	N/A	N/A	N/A	N/A
BAL-002-1	R6.	A Balancing Authority or Reserve Sharing Group shall fully restore its Contingency Reserves within the Contingency Reserve Restoration Period for its Interconnection.	The Balancing Authority or Reserve Sharing Group restored less than 100% but greater than 90% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 90% but greater than 80% of its contingency reserves during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than or equal to 80% but greater than or equal to 70% of its Contingency Reserve during the Contingency Reserve Restoration Period.	The Balancing Authority or Reserve Sharing Group restored less than 70% of its Contingency Reserves during the Contingency Reserve Restoration Period.
BAL-002-1	R6.1.	The Contingency Reserve Restoration Period begins at the end of the Disturbance Recovery Period.	N/A	N/A	N/A	N/A
BAL-002-1	R6.2.	The default Contingency Reserve Restoration Period is 90 minutes.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R1.	Each Balancing Authority shall review its Frequency Bias Settings by January 1 of each year and recalculate its setting to reflect any change in the Frequency Response of the Balancing	The Balancing Authority failed to report the method for determining its Frequency Bias	The Balancing Authority failed to report its Frequency Bias Setting to the NERC Operating	The Balancing Authority failed to report its Frequency Bias Settings and the method for	The Balancing Authority failed to review its Frequency Bias Settings by January 1 of each year

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authority Area.	Setting to the NERC Operating Committee. (R1.2)	Committee. (R1.2)	determining that Frequency Bias Setting to the NERC Operating Committee. (R1.2)	and recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.
BAL-003-0.1b	R1.1.	The Balancing Authority may change its Frequency Bias Setting, and the method used to determine the setting, whenever any of the factors used to determine the current bias value change.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R1.2.	Each Balancing Authority shall report its Frequency Bias Setting, and method for determining that setting, to the NERC Operating Committee.	N/A	N/A	N/A	N/A
BAL-003-0.1b	R2.	Each Balancing Authority shall establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways:	N/A	N/A	N/A	The Balancing Authority established and maintained a Frequency Bias Setting that was less than, the Balancing Authority's Frequency Response.
BAL-003-0.1b	R2.1.	The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours.	N/A	N/A	N/A	The Balancing Authority determination of the fixed Frequency Bias value was not based on observations and averaging the Frequency Response from Disturbances during on-peak hours.
BAL-003-0.1b	R2.2.	The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable	N/A	N/A	N/A	The Balancing Authorities variable frequency bias

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by analyzing Frequency Response as it varies with factors such as load, generation, governor characteristics, and frequency.				maintained was not based on analyses of Frequency Response as it varied with factors such as load, generation, governor characteristics, and frequency.
BAL-003-0.1b	R3.	Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.	N/A	N/A	N/A	The Balancing Authority did not operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, during periods when such operation would not have been adverse to system or Interconnection reliability.
BAL-003-0.1b	R4.	Balancing Authorities that use Dynamic Scheduling or Pseudo-ties for jointly owned units shall reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.	N/A	N/A	N/A	The Balancing Authority that used Dynamic Scheduling or Pseudo-ties for jointly owned units did not reflect its respective share of the unit governor droop response in its respective Frequency Bias Setting.
BAL-003-0.1b	R4.1.	Fixed schedules for Jointly Owned Units mandate that Balancing Authority (A) that contains the Jointly Owned Unit must incorporate the respective share of the unit governor droop response for any Balancing	N/A	N/A	N/A	The Balancing Authority (A) that contained the Jointly Owned Unit with fixed schedules did not incorporate the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authorities that have fixed schedules (B and C). See the diagram below.				respective share of the unit governor droop response for any Balancing Authorities that have fixed schedules (B and C).
BAL-003-0.1b	R4.2.	The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit shall not include their share of the governor droop response in their Frequency Bias Setting. ***See Standard for Graphic***	N/A	N/A	N/A	A Balancing Authority that has a fixed schedule (B and C) but does not contain the Jointly Owned Unit included its share of the governor droop response in its Frequency Bias Setting.
BAL-003-0.1b	R5.	Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that served native load failed to have a monthly average Frequency Bias Setting that was at least 1% of the entities estimated yearly peak demand per 0.1 Hz change.
BAL-003-0.1b	R5.1.	Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.	N/A	N/A	N/A	The Balancing Authority that does not serve native load did not have a monthly average Frequency Bias Setting that was at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.

Complete Violation Severity Level Matrix (BAL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-003-0.1b	R6.	A Balancing Authority that is performing Overlap Regulation Service shall increase its Frequency Bias Setting to match the frequency response of the entire area being controlled. A Balancing Authority shall not change its Frequency Bias Setting when performing Supplemental Regulation Service.	N/A	The Balancing Authority that was performing Overlap Regulation Service changed its Frequency Bias Setting while performing Supplemental Regulation Service.	The Balancing Authority that was performing Overlap Regulation Service failed to increase its Frequency Bias Setting to match the frequency response of the entire area being controlled.	N/A
BAL-004-0	R1.	Only a Reliability Coordinator shall be eligible to act as Interconnection Time Monitor. A single Reliability Coordinator in each Interconnection shall be designated by the NERC Operating Committee to serve as Interconnection Time Monitor.	N/A	N/A	N/A	The responsible entity has designated more than one interconnection time monitor for a single interconnection.
BAL-004-0	R2.	The Interconnection Time Monitor shall monitor Time Error and shall initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.	N/A	N/A	N/A	The responsible entity serving as the Interconnection Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
BAL-004-0	R3.	Each Balancing Authority, when requested, shall participate in a Time Error Correction by one of the following methods:	The Balancing Authority participated in more than 75% and less than 100% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 50% and less than or equal to 75% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in more than 25% and less than or equal to 50% of requested Time Error Corrections for the calendar year.	The Balancing Authority participated in less than or equal to 25% of requested Time Error Corrections for the calendar year.
BAL-004-0	R3.1.	The Balancing Authority shall offset its frequency schedule by 0.02 Hertz,	The Balancing Authority failed to	The Balancing Authority failed to	The Balancing Authority failed to	The Balancing Authority failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		leaving the Frequency Bias Setting normal; or	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 0 to 25% of the time error corrections for the year.	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 25 to 50% of the time error corrections for the year.	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 50 to 75% of the time error corrections for the year.	offset its frequency schedule by 0.02 Hertz and leave their Frequency Bias Setting normal for 75% or more of the time error corrections for the year.
BAL-004-0	R.3.2.	The Balancing Authority shall offset its Net Interchange Schedule (MW) by an amount equal to the computed bias contribution during a 0.02 Hertz Frequency Deviation (i.e. 20% of the Frequency Bias Setting).	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 0 to 25% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 25 to 50% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 50 to 75% of the time error corrections.	The Balancing Authority failed to offset its net interchange schedule frequency schedule by 20% of their frequency bias for 75% or more of the time error corrections.
BAL-004-0	R4.	Any Reliability Coordinator in an Interconnection shall have the authority to request the Interconnection Time Monitor to terminate a Time Error Correction in progress, or a scheduled Time Error Correction that has not begun, for reliability considerations.	N/A	N/A	N/A	The RC serving as the Interconnection Time Monitor failed to initiate or terminate corrective action orders in accordance with the NAESB Time Error Correction Procedure.
BAL-004-0	R4.1.	Balancing Authorities that have reliability concerns with the execution of a Time Error Correction shall notify their Reliability Coordinator and request the termination of a Time Error Correction in progress.	N/A	N/A	N/A	The Balancing Authority with reliability concerns failed to notify the Reliability Coordinator and request the termination of a Time Error Correction in progress.
BAL-005-0.2b	R1.	All generation, transmission, and load operating within an Interconnection	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		must be included within the metered boundaries of a Balancing Authority Area.				
BAL-005-0.2b	R1.1.	Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Generator Operator with generation facilities operating in an Interconnection failed to ensure that those generation facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.2b	R1.2.	Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Transmission Operator with transmission facilities operating in an Interconnection failed to ensure that those transmission facilities were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.2b	R1.3.	Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.	N/A	N/A	N/A	The Load-Serving Entity with load operating in an Interconnection failed to ensure that those loads were included within metered boundaries of a Balancing Authority Area.
BAL-005-0.2b	R2.	Each Balancing Authority shall maintain Regulating Reserve that can	N/A	N/A	N/A	The Balancing Authority failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
	(Retired)	be controlled by AGC to meet the Control Performance Standard.				maintain Regulating Reserve that can be controlled by AGC to meet Control Performance Standard.
BAL-005-0.2b	R3.	A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to ensure adequate metering, communications, and control equipment was provided.
BAL-005-0.2b	R4.	A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority providing Regulation Service failed to notify the Host Balancing Authority for whom it is controlling if it was unable to provide the service, as well as any Intermediate Balancing Authorities.
BAL-005-0.2b	R5.	A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.	N/A	N/A	N/A	The Balancing Authority receiving Regulation Service failed to ensure that back-up plans were in place to provide replacement Regulation Service.
BAL-005-0.2b	R6.	The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its	The Balancing Authority failed to calculate ACE as specified in the	N/A	The Balancing Authority failed to notify the Reliability Coordinator within 30 minutes of its inability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.	inability to calculate ACE.	requirement.		to calculate ACE and failed to use the ACE calculation specified in the requirement in its attempt to calculate ACE.
BAL-005-0.2b	R7.	The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.	N/A	N/A	N/A	The Balancing Authority failed to operate AGC continuously when there were no adverse impacts. OR If its AGC was inoperative the Balancing Authority failed to use manual control to adjust generation to maintain the Net Scheduled Interchange.
BAL-005-0.2b	R8.	The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.	N/A	N/A	N/A	The Balancing Authority failed to ensure that data acquisition for and calculation of ACE occurred at least every six seconds.
BAL-005-0.2b	R8.1.	Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of	N/A	N/A	N/A	The Balancing Authority failed to provide redundant and independent frequency metering equipment that automatically activated upon

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		99.95%.				detection of failure, such that the minimum availability was less than 99.95%.
BAL-005-0.2b	R9.	The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.
BAL-005-0.2b	R9.1.	Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.	N/A	N/A	N/A	The Balancing Authority with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to its Interconnection chose to omit the Interchange Schedule related to the HVDC link from the ACE equation, but failed to model it as internal generation or load.
BAL-005-0.2b	R10.	The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.	N/A	N/A	N/A	The Balancing Authority failed to include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.
BAL-005-0.2b	R11.	Balancing Authorities shall include the effect of Ramp rates, which shall	N/A	N/A	N/A	The Balancing Authority failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.				include the effect of Ramp rates in the Scheduled Interchange values to calculate ACE.
BAL-005-0.2b	R12.	Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.	N/A	N/A	N/A	The Balancing Authority failed to include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.
BAL-005-0.2b	R12.1.	Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.	The Balancing Authority failed to ensure 5% or less of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for 5% or less of the hours.	The Balancing Authority failed to ensure more than 5% up to (and including) 10% of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source. OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for more than 5% up to (and including) 10% of the hours.	The Balancing Authority failed to ensure more than 10% up to (and including) 15% of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source. OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for more than 10% up to (and including) 15% of the hours.	The Balancing Authority failed to ensure more than 15% of all its Tie Line MW metering was telemetered to both control centers and emanates from a common, agreed-upon source. OR The Balancing Authority failed to ensure that megawatt-hour data was telemetered or reported for more than 15% of the hours.
BAL-005-0.2b	R12.2.	Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are	The responsible entity did not ensure that 5% or less of the power flow and ACE signals are not	The responsible entity did not ensure that more than 5% up to (and including) 10% of the power flow and	The responsible entity did not ensure that more than 10% up to (and including) 15% of the power flow and	The responsible entity did not ensure that more than 15% of the power flow and ACE signals are not filtered

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.	filtered except for Anti-aliasing filtering.	ACE signals are not filtered except for Anti-aliasing filtering.	ACE signals are not filtered except for Anti-aliasing filtering.	except for Anti-aliasing filtering.
BAL-005-0.2b	R12.3.	Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.	N/A	N/A	N/A	The applicable entity did not install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented.
BAL-005-0.2b	R13.	Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.	N/A	N/A	N/A	The Balancing Authority failed to perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment OR the Balancing Authority failed to adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (IME) term of the ACE equation to compensate for any equipment error until repairs can be made.
BAL-005-0.2b	R14.	The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation	N/A	N/A	N/A	The Balancing Authority failed to provide its operating personnel with sufficient

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.				instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance.
BAL-005-0.2b	R15.	The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.	N/A	N/A	The Balancing Authority failed to periodically test backup power supplies at the Balancing Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.	The Balancing Authority failed to provide adequate and reliable backup power supplies to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.
BAL-005-0.2b	R16.	The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.	The Balancing Authority failed to collect coincident data to the greatest practical extent.	N/A	The Balancing Authority failed to flag missing or bad data for operator display and archival purposes.	The Balancing Authority failed to sample data at least at the same periodicity with which ACE is calculated.
BAL-005-0.2b	R17.	Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices	N/A	N/A	N/A	The Balancing Authority failed to at least annually check

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below: ***See Standard for Values***				and calibrate its time error and frequency devices against a common reference.
BAL-006-2	R1.	Each Balancing Authority shall calculate and record hourly Inadvertent Interchange.	N/A	N/A	N/A	Each Balancing Authority failed to calculate and record hourly Inadvertent Interchange.
BAL-006-2	R2.	Each Balancing Authority shall include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. The Balancing Authority shall take into account interchange served by jointly owned generators.	N/A	N/A	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. OR Failed to take into account interchange served by jointly owned generators.	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. AND Failed to take into account interchange served by jointly owned generators.
BAL-006-2	R3.	Each Balancing Authority shall ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority failed to ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Balancing Authorities.
BAL-006-2	R4.	Adjacent Balancing Authority Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign. Each Balancing Authority shall compute its Inadvertent Interchange based on the following:	The Balancing Authority failed to record Actual Net Interchange values that are equal but opposite in sign to its Adjacent Balancing Authorities.	The Balancing Authority failed to compute Inadvertent Interchange.	The Balancing Authority failed to operate to a common Net Interchange Schedule that is equal but opposite to its Adjacent Balancing Authorities.	N/A
BAL-006-2	R4.1	Each Balancing Authority, by the end of the next business day, shall agree with its Adjacent Balancing Authorities to:	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net Interchanged Schedule. AND The hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-2	R4.1.1.	The hourly values of Net Interchange Schedule.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net Interchanged Schedule.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
BAL-006-2	R4.1.2.	The hourly integrated megawatt-hour values of Net Actual Interchange.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly integrated megawatt-hour values of Net Actual Interchange.
BAL-006-2	R4.2.	Each Balancing Authority shall use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.	N/A	N/A	N/A	The Balancing Authority failed to use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.
BAL-006-2	R4.3.	A Balancing Authority shall make after-the-fact corrections to the agreed-to daily and monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). Changes or corrections based on non-reliability considerations shall not be reflected in the Balancing Authority's Inadvertent Interchange. After-the-fact corrections to scheduled or actual values will not be accepted without agreement of the Adjacent Balancing Authority(ies).	N/A	N/A	N/A	The Balancing Authority failed to make after-the-fact corrections to the agreed-to daily and monthly accounting data to reflect actual operating conditions or changes or corrections based on non-reliability considerations were reflected in the Balancing Authority's Inadvertent Interchange.
BAL-006-2	R5.	Adjacent Balancing Authorities that	Adjacent Balancing	Adjacent Balancing	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cannot mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month shall, for the purposes of dispute resolution, submit a report to their respective Regional Reliability Organization Survey Contact. The report shall describe the nature and the cause of the dispute as well as a process for correcting the discrepancy.	Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities, submitted a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute but failed to provide a process for correcting the discrepancy.	Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month, failed to submit a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute as well as a process for correcting the discrepancy.		
BAL-502-RFC-02	R1.	The Planning Coordinator shall perform and document a Resource Adequacy analysis annually. The Resource Adequacy analysis shall: *[See standard pdf for sub-requirements]*	The Planning Coordinator Resource Adequacy analysis failed to consider 1 or 2 of the Resource availability characteristics subcomponents under R1.4 and documentation of how and why they were included in the analysis or why they were not included OR The Planning	The Planning Coordinator Resource Adequacy analysis failed to express the planning reserve margin developed from R1.1 as a percentage of the net Median forecast peak Load per R1.1.2 OR The Planning Coordinator Resource Adequacy analysis failed to include 1 of the Load forecast Characteristics	The Planning Coordinator Resource Adequacy analysis failed to be performed or verified separately for individual years of Year One through Year Ten per R1.2 OR The Planning Coordinator failed to perform an analysis or verification for one year in the 2 through 5 year period or one year in the 6 though 10 year	The Planning Coordinator failed to perform and document a Resource Adequacy analysis annually per R1. OR The Planning Coordinator Resource Adequacy analysis failed to calculate a Planning reserve margin that will result in the sum of the probabilities for loss of Load for the integrated

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Coordinator Resource Adequacy analysis failed to consider Transmission maintenance outage schedules and document how and why they were included in the analysis or why they were not included per R1.5	subcomponents under R1.3.1 and documentation of its use OR The Planning Coordinator Resource Adequacy analysis failed to include 1 of the Resource Characteristics subcomponents under R1.3.2 and documentation of its use Or The Planning Coordinator Resource Adequacy analysis failed to document that all Load in the Planning Coordinator area is accounted for in its Resource Adequacy analysis per R1.7	period or both per R1.2.2 OR The Planning Coordinator Resource Adequacy analysis failed to include 2 or more of the Load forecast Characteristics subcomponents under R1.3.1 and documentation of their use OR The Planning Coordinator Resource Adequacy analysis failed to include 2 or more of the Resource Characteristics subcomponents under R1.3.2 and documentation of their use OR The Planning Coordinator Resource Adequacy analysis failed to include Transmission	peak hour for all days of each planning year analyzed for each planning period being equal to 0.1 per R1.1 OR The Planning Coordinator failed to perform an analysis for Year One per R1.2.1

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					limitations and documentation of its use per R1.3.3 OR The Planning Coordinator Resource Adequacy analysis failed to include assistance from other interconnected systems and documentation of its use per R1.3.4 OR The Planning Coordinator Resource Adequacy analysis failed to consider 3 or more Resource availability characteristics subcomponents under R1.4 and documentation of how and why they were included in the analysis or why they were not included OR The Planning Coordinator Resource	

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					Adequacy analysis failed to document that capacity resources are appropriately accounted for in its Resource Adequacy analysis per R1.6	
BAL-502-RFC-02	R2.	The Planning Coordinator shall annually document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis. *[See standard pdf for sub-requirements]*	The Planning Coordinator failed to publicly post the documents as specified per requirement R2.1 and R2.2 later than 30 calendar days prior to the beginning of Year One per R2.3	The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis for one of the years in the 2 through 10 year period per R2.1. OR The Planning Coordinator failed to document the Planning Reserve margin calculated per requirement R1.1 for each of the three years in the analysis per R2.2.	The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis for year 1 of the 10 year period per R2.1. OR The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis for two or more of the years in the 2 through 10 year period per R2.1.	The Planning Coordinator failed to document the projected Load and resource capability, for each area or Transmission constrained sub-area identified in the Resource Adequacy analysis per R2.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-001-2a	R1.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.	N/A	N/A	The responsible entity has procedures for the recognition of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection but does not have a procedure for making their operating personnel aware of said events.	The responsible entity failed to have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.
CIP-001-2a	R2.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	N/A	N/A	The responsible entity has demonstrated the existence of a procedure to communicate information concerning sabotage events, but not all of the appropriate parties in the interconnection are identified.	The responsible entity failed to have a procedure for communicating information concerning sabotage events.
CIP-001-2a	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to	N/A	The responsible entity provided its operating personnel with a sabotage response guideline, but failed to include the personnel to contact for reporting disturbances due to	N/A	The responsible entity failed to provide its operating personnel with a sabotage response guideline.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		sabotage events.		sabotage events.		
CIP-001-2a	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	N/A	N/A	The responsible entity has established communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, but has not developed a reporting procedure.	The responsible entity failed to establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials, and has not developed a reporting procedure.
CIP-002-3	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
CIP-002-3	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
CIP-002-3	R1.2	The risk-based assessment shall consider the following assets:	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R1.2.1 through R1.2.7 in its risk-based assessment.
CIP-002-3	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.4.	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	N/A	N/A	N/A	N/A
CIP-002-3	R1.2.7.	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	N/A	N/A	N/A	N/A
CIP-002-3	R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has	The Responsible Entity did not develop a list of its identified Critical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.			not been reviewed and updated annually as required.	Assets even if such list is null.
CIP-002-3	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null.
CIP-002-3	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R3.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
CIP-002-3	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)
CIP-002-4	R1.		N/A	N/A	The Responsible	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.			Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. For the purpose of Standard CIP-002-4, Critical Cyber Assets are	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.				Asset List.
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-3	R1.	Cyber Security Policy — The Responsible Entity shall document and	N/A	N/A	N/A	The Responsible Entity has not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:				documented or implemented a cyber security policy.
CIP-003-3	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-3	R1.2. (Retired)	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-3	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-3	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		through CIP-009-3.				leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-3	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-3	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-3	R2.3.	Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					are not documented within thirty calendar days of the effective date.	within thirty calendar days of the effective date.
CIP-003-3	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-3	R3. (Retired)	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were not documented.
CIP-003-3	R3.1. (Retired)	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).
CIP-003-3	R3.2. (Retired)	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-3	R3.3. (Retired)	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed or were not approved on an annual basis by the senior manager or delegate(s) to ensure the exceptions are still required and valid or the review and approval is not documented.
CIP-003-3	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-3	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP- 002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans,	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		incident response plans, and security configuration information.				
CIP-003-3	R4.2. (Retired)	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-3	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-3	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-3	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-3	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, and the information for which they are responsible for authorizing access, but the business phone is missing.	Personnel are not identified by name, title, or the information for which they are responsible for authorizing access.
CIP-003-3	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-3	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						needs and appropriate personnel roles and responsibilities.
CIP-003-3	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-3	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-003-4	R1.	Cyber Security Policy —The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
CIP-003-4	R1.2. (Retired)	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-4	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
CIP-003-4	R2.	Leadership —The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R2.4.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-4	R3. (Retired)	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
CIP-003-4	R3.1. (Retired)	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
CIP-003-4	R3.2. (Retired)	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating	N/A	N/A	The Responsible Entity has a documented exception to the	The Responsible Entity has a documented exception to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		measures.			cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-4	R3.3. (Retired)	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
CIP-003-4	R4.	Information Protection —The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-4	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar	N/A	N/A	The information protection program does not include one of the minimum information types to	The information protection program does not include two or more of the minimum

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.			be protected as detailed in R4.1.	information types to be protected as detailed in R4.1.
CIP-003-4	R4.2. (Retired)	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-4	R5.	Access Control —The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	The Responsible Entity implemented but did not document a program for managing access to protected	The Responsible Entity documented but did not implement a program for managing access	The Responsible Entity did not implement nor document a program for managing access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Critical Cyber Asset information.	to protected Critical Cyber Asset information.	to protected Critical Cyber Asset information.
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-4	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		roles and responsibilities.				privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-4	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	The Responsible Entity has established but not documented a change control process OR The Responsible Entity has established but not documented a configuration management process.	The Responsible Entity has established but not documented both a change control process and configuration management process.	The Responsible Entity has not established and documented a change control process OR The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a change control process AND The Responsible Entity has not established and documented a configuration management process.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-3	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	N/A	N/A	The Responsible[1] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
CIP-004-3	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be	N/A	N/A	The Responsible[2] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		updated whenever necessary.				physical access to Critical Cyber Assets.
CIP-004-3	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A	N/A	N/A	Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-3	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-3	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-3	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-3	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but	The Responsible Entity did not maintain documentation that training is conducted

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					did not include attendance records.	at least annually, including the date the training was completed and attendance records.
CIP-004-3	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R3, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, as stated in R3, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-004-3	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		criticality of the position.			in the U.S.) or a seven-year criminal check.	in the U.S.) and seven-year criminal check.
CIP-004-3	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-3	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-3	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 15% or more of the authorized personnel.
CIP-004-3	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-3	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						longer require such access to Critical Cyber Assets.
CIP-004-4	R1.	Awareness —The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g., emails, memos, computer based training, etc.); • Indirect communications (e.g., posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
CIP-004-4	R2.	Training —The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to	The Responsible Entity did not establish, document, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access to Critical Cyber Assets.		Critical Cyber Assets.	Critical Cyber Assets.
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-4	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.
CIP-004-4	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	such personnel were granted such access except in specified circumstances such as an emergency.	existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-4	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				update it for cause when applicable.	after the initial personnel risk assessment.	assessment nor was it updated for cause when applicable.
CIP-004-4	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.
CIP-004-4	R4.	Access —The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets,	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 10% or more	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 15% or more

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			missing at least one individual but less than 5% of the authorized personnel.		but less than 15% of the authorized personnel.	of the authorized personnel.
CIP-004-4	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-4	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-3a	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-3a	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-3a	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the dial-up device.
CIP-005-3a	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-3a	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-3a	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-	N/A	N/A	N/A	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded one (1) or more of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		009-3.				Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3c Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.
CIP-005-3a	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of one or more of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
CIP-005-3a	R2.	Electronic Access Controls — The Responsible Entity shall implement and	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).				implement or did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005-3a	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-3a	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	N/A	N/A	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						services.
CIP-005-3a	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-3a	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-3a	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-3a	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-3a	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-3a	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		004-3 Requirement R4.				
CIP-005-3a	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-3a	R2.6. (Retired)	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
CIP-005-3a	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-3a	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						monitoring at one or more access points to dial-up devices.
CIP-005-3a	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR The above alerts do not provide for appropriate notification to designated response personnel. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
CIP-005-3a	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerability assessment shall include, at a minimum, the following:				annually for one or more of the access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-3a	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-3a	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-005-3a	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			5% of the documentation to support compliance with the requirements of Standard CIP-005.	documentation to support compliance with the requirements of Standard CIP-005.	documentation to support compliance with the requirements of Standard CIP-005.	with the requirements of Standard CIP-005.
CIP-005-3a	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-3a	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-3a	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-005-4a	R1.	Electronic Security Perimeter —The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and	The Responsible Entity did not document one or more access points to the Electronic	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Security Perimeter(s).		an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
CIP-005-4a	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-4a	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
CIP-005-4a	R1.3.	Communication links connecting	N/A	N/A	N/A	At least one end point

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).				of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-4a	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-4a	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
CIP-005-4a	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-4a	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005-4a	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-4a	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document,	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Perimeter.	individually or by specified grouping, the configuration of those ports and services.	individually or by specified grouping, the configuration of those ports and services.
CIP-005-4a	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-4a	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-4a	R2.5.	The required documentation shall, at least, identify and describe:	The required documentation for R2 did not include one of the elements described in R2.5.1 through	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			R2.5.4			
CIP-005-4a	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-4a	R2.6. (Retired)	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			appropriate use banner on the user screen upon all interactive access attempts.			
CIP-005-4a	R3.	Monitoring Electronic Access —The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
CIP-005-4a	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			manual processes for monitoring at less than 5% of the access points to dial-up devices.			
CIP-005-4a	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate notification to designated response personnel.	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
CIP-005-4a	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-4a	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-4a	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-005-4a	R5.	Documentation Review and Maintenance —The Responsible Entity shall review, update, and maintain all documentation to support compliance with the	The Responsible Entity did not review, update, and maintain at	The Responsible Entity did not review, update, and maintain greater than 5% but	The Responsible Entity did not review, update, and maintain greater than 10% but	The Responsible Entity did not review, update, and maintain greater than 15% of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		requirements of Standard CIP-005-4a.	least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	the documentation to support compliance with the requirements of Standard CIP-005-4.
CIP-005-4a	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
CIP-005-4a	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
CIP-005-4a	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable	The Responsible Entity retained electronic access	The Responsible Entity retained electronic access logs	The Responsible Entity retained electronic access logs	The Responsible Entity retained electronic access logs

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	logs for 75 or more calendar days, but for less than 90 calendar days.	for 60 or more calendar days, but for less than 75 calendar days.	for 45 or more calendar days , but for less than 60 calendar days.	for less than 45 calendar days.
CIP-006-3c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
CIP-006-3c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall")

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						border cannot be established, the Responsible Entity has not deployed or documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-3c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter or does not identify measures to control entry at those access points.
CIP-006-3c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-3c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-3c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the review of access authorization requests or the revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
CIP-006-3c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A	N/A	N/A	The Responsible Entity did not include or implement a visitor control program in its physical security plan or it does not meet the requirements of continuous escort.
CIP-006-3c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-3c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-3c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address r updating the physical security plan within thirty calendar days of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access controls, monitoring controls, or logging controls.				completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration
CIP-006-3c	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-3c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A	N/A	N/A	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was not afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.
CIP-006-3c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-3c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	N/A	N/A	N/A	N/A
CIP-006-3c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) does not reside within an identified Physical Security Perimeter.
CIP-006-3c	R4	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the	N/A	N/A	N/A	The Responsible Entity has not documented or has not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets				more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-3c	R5	Monitoring Physical Access — The Responsible Entity shall document and	N/A	N/A.	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.				Entity has not documented or has not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-3.
CIP-006-3c	R6	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of		N/A	N/A	The Responsible Entity has not implemented or has not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4				control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-3c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	N/A	N/A	N/A	The responsible entity did not retain physical access logs for at least ninety calendar days.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-006-3c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-3c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-3c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-3c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.	Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR	The Responsible Entity did not document, implement, and maintain a physical security plan.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity created and implemented but did not maintain a physical security plan.	
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Security Perimeter.	entry at those access points.	entry at those access points.
CIP-006-4c	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-4c	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-4c	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.
CIP-006-4c	R1.6.	A visitor control program for visitors (personnel without authorized unescorted	The responsible Entity included a	The responsible Entity included a visitor	The responsible Entity included a	The Responsible Entity did not include

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access to a Physical Security Perimeter), containing at a minimum the following:	visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.	control program in its physical security plan, but either did not log the visitor or did not log the escort.	visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	or implement a visitor control program in its physical security plan.
CIP-006-4c	R1.6.1.	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.6.2.	Continuous escorted access of visitors within the Physical Security Perimeter.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or reconfiguration.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					reconfiguration.	
CIP-006-4c	R1.8.	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical Security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-4c	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP- 009-4.		Standard CIP-009-4.	point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	N/A	N/A	N/A	N/A
CIP-006-4c	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						an identified Physical Security Perimeter.
CIP-006-4c	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	N/A	The Responsible Entity has implemented but not documented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. Security Personnel: Personnel responsible for controlling	The Responsible Entity has documented but not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel:	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets..
CIP-006-4c	R5.	Monitoring Physical Access —The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access points by authorized personnel as specified in Requirement R4.		personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-4.
CIP-006-4c	R6.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week..	control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.
CIP-006-4c	R7.	Access Log Retention —The Responsible Entity shall retain physical access logs for at least ninety calendar	The Responsible Entity retained physical access	The Responsible Entity retained physical access logs	The Responsible Entity retained physical access logs	The Responsible Entity retained physical access logs

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	logs for 75 or more calendar days, but for less than 90 calendar days.	for 60 or more calendar days, but for less than 75 calendar days.	for 45 or more calendar days, but for less than 60 calendar days.	for less than 45 calendar days.
CIP-006-4c	R8.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
CIP-006-4c	R8.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-3	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	N/A	N/A	N/A	The Responsible Entity did not ensure the prevention of adverse affects described in R1, by not including the required minimum significant changes. OR The Responsible Entity did not address one or more of the following: R1.1, R1.2, R1.3.
CIP-007-3	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	N/A	N/A	N/A	N/A
CIP-007-3	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-3	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-3	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-3	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk.
CIP-007-3	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document, either separately or as a component of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).				documented configuration management process specified in CIP-003-3 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-3	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-3	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk.
CIP-007-3	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-3	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-3	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	N/A	N/A	N/A	The Responsible Entity did not document or did not implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-3	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	N/A	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-3	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						know" with respect to work functions performed.
CIP-007-3	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-3	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-3	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
CIP-007-3	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.				implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-3	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-3	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-3	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity has not implemented (one or more components of) a policy for managing the use of such accounts that limits

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-3	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity does not require passwords subject to R5.3.1, R5.3.2, R5.3.3. OR Does not use passwords subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-3	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-3	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-3	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-3	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to	N/A	N/A	N/A	The Responsible Entity as technically feasible, did not implement automated tools or organizational

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitor system events that are related to cyber security.				process controls, to monitor system events that are related to cyber security on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-3	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
CIP-007-3	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-3	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						incident response as required in Standard CIP-008.
CIP-007-3	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-3	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-3	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.	N/A	N/A	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005- 3 but did not address redeployment as specified in R7.2.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3. OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2 but did not address disposal as specified in R7.1. ~~OR~~ ~~The Responsible Entity did not maintain records pertaining to disposal or~~[3] ~~redeployment as specified in R7.3.~~

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						(Deleted text retired)
CIP-007-3	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-3	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-3	R7.3. (Retired)	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-3	R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment on one or more Cyber Assets within the Electronic Security Perimeter at least annually. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
CIP-007-3	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-3	R8.2.	A review to verify that only ports and services required for operation of the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Cyber Assets within the Electronic Security Perimeter are enabled;				
CIP-007-3	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-3	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-007-3	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-3 at least annually and changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.
CIP-007-4	R1.	Test Procedures —The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not	N/A	The Responsible Entity did create, implement and maintain the test procedures as required	The Responsible Entity did not create, implement and maintain the test procedures as	The Responsible Entity did not create, implement and maintain the test procedures as

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.		in R1.1, but did not document that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	required in R1.1.	required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
CIP-007-4	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	N/A	N/A	N/A	N/A
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-4	R2.	Ports and Services —The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Entity did not document compensating measure(s) applied to mitigate risk exposure.
CIP-007-4	R3.	Security Patch Management —The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within	The Responsible Entity documented the assessment of	The Responsible Entity documented the assessment of security	The Responsible Entity documented the assessment of	The Responsible Entity documented the assessment of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		thirty calendar days of availability of the patches or upgrades.	security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.
CIP-007-4	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
CIP-007-4	R4.	Malicious Software Prevention —The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware")	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Security Perimeter(s).	prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-4	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	The Responsible Entity, as technically feasible, documented and implemented a	The Responsible Entity, as technically feasible, did not document but implemented a process, including	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-4	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-4	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.	At least one user account but less than 1% of user accounts	One (1) % or more of user accounts but less than 3% of user accounts implemented	Three (3) % or more of user accounts but less than 5% of user accounts	Five (5) % or more of user accounts implemented by the Responsible Entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			implemented by the Responsible Entity, were not approved by designated personnel.	by the Responsible Entity were not approved by designated personnel.	implemented by the Responsible Entity were not approved by designated personnel.	were not approved by designated personnel.
CIP-007-4	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
CIP-007-4	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						account privileges including factory default accounts.
CIP-007-4	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-4	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization,	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization,	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		risk.				
CIP-007-4	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-4	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.

Complete Violation Severity Level Matrix (CIP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 but did not maintain records as specified in R7.3. (Retired)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
CIP-007-4	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-4	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R7.3. (Retired)	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-4	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-4	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	N/A	N/A	N/A	N/A
CIP-007-4	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-007-4	R9.	Documentation Review and Maintenance —The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually nor were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.
CIP-008-3	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					components.	Cyber Security Incident.
CIP-008-3	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-3	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-3	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	N/A	N/A	N/A	N/A
CIP-008-3	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	N/A	N/A	N/A	N/A
CIP-008-3	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-3	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-3	R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		years.				Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-008-4	R1.	Cyber Security Incident Response Plan —The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-4	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	N/A	N/A	N/A	N/A
CIP-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		calendar days of any changes.				
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-4	R2.	Cyber Security Incident Documentation —The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for two but less than three calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than two calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than one calendar year.	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1.
CIP-009-3	R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	N/A	N/A	N/A	The Responsible Entity has not created or has not annually reviewed their recovery plan(s) for Critical Cyber Assets OR has created a plan but did not address one or more of the requirements CIP-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						009-1 R1.1 and R1.2.
CIP-009-3	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-3	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-3	R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-3	R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were not communicated to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change.
CIP-009-3	R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-3	R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.
CIP-009-4	R1.	Recovery Plans —The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	N/A	The Responsible Entity has not annually reviewed recovery plan(s) for Critical Cyber Assets.	The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP-009-4 R1.1 or R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-4 R1.1 and R1.2.
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the recovery plan(s).				
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-4	R2.	Exercises —The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-4	R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementation of the recovery plan(s) in more than 180 calendar days of the change.
CIP-009-4	R4.	Backup and Restore —The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-4	R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
COM-001-1.1	R1.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:	N/A	The responsible entity failed to provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information to one of the groups specified in R1.1, or R1.2, or R1.3	The responsible entity failed to provide adequate and reliable telecommunications facilities for the exchange of Interconnection or operating information to two of the groups specified in R1.1, or R1.2, or R1.3.	The responsible entity failed to provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information to all 3 of the groups specified in R1.1, or R1.2, or R1.3. OR The responsible entity's telecommunications is not redundant or diversely routed as applicable as specified in R1.4
COM-001-1.1	R1.1.	Internally.	N/A	N/A	N/A	N/A
COM-001-1.1	R1.2.	Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	N/A
COM-001-1.1	R1.3.	With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.	N/A	N/A	N/A	N/A
COM-001-1.1	R1.4.	Where applicable, these facilities shall be redundant and diversely routed.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
COM-001-1.1	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.	N/A	The responsible entity failed to give special attention to emergency telecommunications facilities and equipment not used for routine communications.	N/A	The responsible entity failed to manage, alarm, test and/or actively monitor its vital telecommunications facilities.
COM-001-1.1	R3.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.	N/A	N/A	The responsible entity failed to assist in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.	The responsible entity failed to provide a means to coordinate telecommunications among their respective areas including assisting in the investigation and recommending of solutions to telecommunications problems within the area and with other areas.
COM-001-1.1	R4.	Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing Authorities may use an alternate language for internal operations.	N/A	N/A	N/A	The responsible entity used a language other than English and failed to have an agreement to do so.
COM-001-	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing	N/A	N/A	N/A	The responsible entity did not have

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
1.1		Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.				written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.
COM-001-1.1	R6.	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, “NERCNet Security Policy.”	The NERCNet User Organization failed to adhere to 5% or less of the requirements listed in Attachment 1-COM-001, , "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to more than 5% up to (and including) 10% of the requirements listed in Attachment 1 - COM-001, "NERCNet Security Policy".	The NERCNet User Organization failed to adhere to more than 10% up to (and including) 15% of the requirements listed in Attachment 1-COM-001 "NERCNet Security Policy".	The NERCNet User Organization failed to more than 15% of the requirements listed in Attachment 1-COM-001, "NERCNet Security Policy".
COM-002-2	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.	N/A	The responsible entity did not have data links with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. OR The responsible entity did not have voice links with appropriate Reliability Coordinators, Balancing Authorities, and	N/A	The responsible entity failed to have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. OR The responsible entity's communications were not staffed and available for addressing real time emergency

Complete Violation Severity Level Matrix (COM)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Transmission Operators.		conditions.
COM-002-2	R1.1.	Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.	N/A	N/A	The responsible entity failed to notify all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding was anticipated.	The responsible entity failed to notify its Reliability Coordinator through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding was anticipated.
COM-002-2	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall issue directives in a clear, concise, and definitive manner; shall ensure the recipient of the directive repeats the information back correctly; and shall acknowledge the response as correct or repeat the original statement to resolve any misunderstandings.	N/A	The responsible entity provided a clear directive in a clear, concise and definitive manner and required the recipient to repeat the directive, but did not acknowledge the recipient was correct in the repeated directive.	The responsible entity provided a clear directive in a clear, concise and definitive manner, but did not require the recipient to repeat the directive.	The responsible entity failed to provide a clear directive in a clear, concise and definitive manner when required.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-001-0.1b	R1.	Balancing Authorities shall have operating agreements with adjacent Balancing Authorities that shall, at a minimum, contain provisions for emergency assistance, including provisions to obtain emergency assistance from remote Balancing Authorities.	N/A	The Balancing Authority demonstrated the existence of an operating agreement with at least one adjacent Balancing Authority for emergency assistance, but the agreement did not include provision for obtaining emergency assistance from any remote Balancing Authority.	N/A	The Balancing Authority did not demonstrate the existence of any operating agreements with adjacent Balancing Authorities that include provision for emergency assistance with adjacent Balancing Authorities.
EOP-001-0.1b	R2.	The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. The plan shall include the details on how the Transmission Operator will implement load reduction in sufficient amount and time to mitigate the IROL violation before system separation or collapse would occur. The load reduction plan must be capable of being implemented within 30 minutes.	N/A	N/A	The Transmission Operator demonstrated the existence of an emergency load reduction plan for each identified IROL but at least one of the plans will take longer than 30 minutes to implement.	The Transmission Operator failed to demonstrate the existence of an emergency load reduction plan for all identified IROLs.
EOP-001-0.1b	R3.	Each Transmission Operator and Balancing Authority shall:	N/A	N/A	N/A	N/A
EOP-001-0.1b	R3.1.	Develop, maintain, and implement a set of plans to mitigate operating emergencies for insufficient generating capacity.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating emergencies for insufficient	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans to mitigate operating emergencies

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				emergencies for insufficient generating capacity and the plans are implemented but the plans are not maintained.	generating capacity but the plans are neither maintained nor implemented.	for insufficient generating capacity.
EOP-001-0.1b	R3.2.	Develop, maintain, and implement a set of plans to mitigate operating emergencies on the transmission system.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating emergencies on the transmission system and the plans are implemented but the plans are not maintained.	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans to mitigate operating emergencies on the transmission system but the plans are neither maintained nor implemented.	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans to mitigate operating emergencies on the transmission system.
EOP-001-0.1b	R3.3.	Develop, maintain, and implement a set of plans for load shedding.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for load shedding and the plans are implemented but the plans are not maintained.	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for load shedding but the plans are neither maintained nor implemented.	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans for load shedding.
EOP-001-0.1b	R3.4.	Develop, maintain, and implement a set of plans for system restoration.	N/A	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for system restoration and the	The Transmission Operator or Balancing Authority demonstrated the existence of a set of plans for system restoration but the plans are neither maintained	The Transmission Operator or Balancing Authority failed to demonstrate the existence of a set of plans for system restoration.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				plans are implemented but the plans are not maintained.	nor implemented.	
EOP-001-0.1b	R4.	Each Transmission Operator and Balancing Authority shall have emergency plans that will enable it to mitigate operating emergencies. At a minimum, Transmission Operator and Balancing Authority emergency plans shall include:	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans do not include sub-requirement R4.4.	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans do not include sub-requirement R4.3.	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans do not include either sub-requirement R4.1 or R4.2.	The Transmission Operator or Balancing Authority demonstrated the existence of emergency plans that will enable it to mitigate operating emergencies but the plans are missing two (2) or more of the sub-requirements identified for R4.
EOP-001-0.1b	R4.1.	Communications protocols to be used during emergencies.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R4.2.	A list of controlling actions to resolve the emergency. Load reduction, in sufficient quantity to resolve the emergency within NERC-established timelines, shall be one of the controlling actions.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R4.3.	The tasks to be coordinated with and among adjacent Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R4.4.	Staffing levels for the emergency.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R5.	Each Transmission Operator and Balancing Authority shall include the applicable elements in Attachment 1-EOP-001 when developing an emergency plan.	The Transmission Operator and Balancing Authority emergency plan has complied with 90% or more of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 70% to 90% of the number of sub-	The Transmission Operator and Balancing Authority emergency plan has complied with between 50% to 70% of the number of sub-components.	The Transmission Operator and Balancing Authority emergency plan has complied with 50% or less of the number of sub-components

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				components.		
EOP-001-0.1b	R6.	The Transmission Operator and Balancing Authority shall annually review and update each emergency plan. The Transmission Operator and Balancing Authority shall provide a copy of its updated emergency plans to its Reliability Coordinator and to neighboring Transmission Operators and Balancing Authorities.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to provide evidence that it completed an annual review, and updated each of its emergency plans appropriately. OR The Transmission Operator or Balancing Authority failed to provide a copy of one of its updated emergency plans to its Reliability Coordinator, all its neighboring Transmission Operators, and all its neighboring Balancing Authorities.
EOP-001-0.1b	R7.	The Transmission Operator and Balancing Authority shall coordinate its emergency plans with other Transmission Operators and Balancing Authorities as appropriate. This coordination includes the following steps, as applicable:	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in R7.4 was applicable and was not included.	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in R7.3 was applicable and	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in either R7.1 or R7.2 was applicable and was not included. .	The Transmission Operator or Balancing Authority demonstrated that it coordinated its emergency plans with other Transmission Operators and Balancing Authorities as appropriate but the coordination specified in two (2) or more of the sub-requirements was applicable and was not included.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				was not included.		
EOP-001-0.1b	R7.1.	The Transmission Operator and Balancing Authority shall establish and maintain reliable communications between interconnected systems.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R7.2.	The Transmission Operator and Balancing Authority shall arrange new interchange agreements to provide for emergency capacity or energy transfers if existing agreements cannot be used.	N/A	N/A	N/A	N/A
EOP-001-0.1b	R7.3.	The Transmission Operator and Balancing Authority shall coordinate transmission and generator maintenance schedules to maximize capacity or conserve the fuel in short supply. (This includes water for hydro generators.)	N/A	N/A	N/A	N/A
EOP-001-0.1b	R7.4.	The Transmission Operator and Balancing Authority shall arrange deliveries of electrical energy or fuel from remote systems through normal operating channels.	N/A	N/A	N/A	N/A
EOP-002-3.1	R1.	Each Balancing Authority and Reliability Coordinator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area and shall exercise specific authority to alleviate capacity and energy emergencies.	N/A	N/A	N/A	The Balancing Authority or Reliability Coordinator does not have responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area OR The Balancing Authority or Reliability Coordinator did not exercise its authority

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						to alleviate capacity and energy emergencies.
EOP-002-3.1	R2.	Each Balancing Authority shall, when required and as appropriate, take one or more actions as described in its capacity and energy emergency plan, to reduce risks to the interconnected system.	N/A	N/A	N/A	The Balancing Authority did not implement its capacity and energy emergency plan, when required and as appropriate, to reduce risks to the interconnected system.
EOP-002-3.1	R3.	A Balancing Authority that is experiencing an operating capacity or energy emergency shall communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.	N/A	N/A	The Balancing Authority communicated its current and future system conditions to its Reliability Coordinator but did not communicate to one or more of its neighboring Balancing Authorities.	The Balancing Authority has failed to communicate its current and future system conditions to its Reliability Coordinator and neighboring Balancing Authorities.
EOP-002-3.1	R4.	A Balancing Authority anticipating an operating capacity or energy emergency shall perform all actions necessary including bringing on all available generation, postponing equipment maintenance, scheduling interchange purchases in advance, and being prepared to reduce firm load.	N/A	N/A	N/A	The Balancing Authority has failed to perform the necessary actions as required and stated in the requirement.
EOP-002-3.1	R5.	A deficient Balancing Authority shall only use the assistance provided by the Interconnection's frequency bias for the time needed to implement corrective actions. The Balancing Authority shall not unilaterally adjust generation in an attempt to return Interconnection frequency to	N/A	N/A	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement corrective	The Balancing Authority used the assistance provided by the Interconnection's frequency bias for more time than needed to implement

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		normal beyond that supplied through frequency bias action and Interchange Schedule changes. Such unilateral adjustment may overload transmission facilities.			actions.	corrective actions and unilaterally adjust generation in an attempt to return Interconnection frequency to normal beyond that supplied through frequency bias action and Interchange Schedule changes.
EOP-002-3.1	R6.	If the Balancing Authority cannot comply with the Control Performance and Disturbance Control Standards, then it shall immediately implement remedies to do so. These remedies include, but are not limited to:	The Balancing Authority failed to comply with one of the sub-components.	The Balancing Authority failed to comply with 2 of the sub-components.	The Balancing Authority failed to comply with 3 of the sub-components.	The Balancing Authority failed to comply with more than 3 of the sub-components.
EOP-002-3.1	R6.1.	Loading all available generating capacity.	N/A	N/A	N/A	The Balancing Authority did not use all available generating capacity.
EOP-002-3.1	R6.2.	Deploying all available operating reserve	N/A	N/A	N/A	The Balancing Authority did not deploy all of its available operating reserve.
EOP-002-3.1	R6.3.	Interrupting interruptible load and exports.	N/A	N/A	N/A	The Balancing Authority did not interrupt interruptible load and exports.
EOP-002-3.1	R6.4.	Requesting emergency assistance from other Balancing Authorities.	N/A	N/A	N/A	The Balancing Authority did not request emergency assistance from other Balancing Authorities.
EOP-002-3.1	R6.5.	Declaring an Energy Emergency through its	N/A	N/A	N/A	The Balancing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinator; and				Authority did not declare an Energy Emergency through its Reliability Coordinator.
EOP-002-3.1	R6.6.	Reducing load, through procedures such as public appeals, voltage reductions, curtailing interruptible loads and firm loads.	N/A	N/A	N/A	The Balancing Authority did not implement one or more of the procedures stated in the requirement.
EOP-002-3.1	R7.	Once the Balancing Authority has exhausted the steps listed in Requirement 6, or if these steps cannot be completed in sufficient time to resolve the emergency condition, the Balancing Authority shall:	N/A	N/A	The Balancing Authority has met only one of the two requirements	The Balancing Authority has not met either of the two requirements
EOP-002-3.1	R7.1.	Manually shed firm load without delay to return its ACE to zero; and	N/A	N/A	N/A	The Balancing Authority did not manually shed firm load without delay to return it's ACE to zero.
EOP-002-3.1	R7.2.	Request the Reliability Coordinator to declare an Energy Emergency Alert in accordance with Attachment 1-EOP-002 "Energy Emergency Alerts."	The Balancing Authority's implementation of an Energy Emergency Alert has missed minor program/procedural elements in Attachment 1-EOP-002-0.	N/A	N/A	The Balancing Authority has failed to meet one or more of the requirements of Attachment 1-EOP-002-0.
EOP-002-3.1	R8.	A Reliability Coordinator that has any Balancing Authority within its Reliability Coordinator area experiencing a potential or actual Energy Emergency shall initiate an Energy Emergency Alert as detailed in	The Reliability Coordinator's implementation of an Energy Emergency Alert has missed	N/A	N/A	The Reliability Coordinator has failed to meet one or more of the requirements of Attachment 1-EOP-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1-EOP-002 "Energy Emergency Alerts." The Reliability Coordinator shall act to mitigate the emergency condition, including a request for emergency assistance if required.	minor program/procedural elements in Attachment 1-EOP-002-0.			002-0.
EOP-002-3.1	R9.	When a Transmission Service Provider expects to elevate the transmission service priority of an Interchange Transaction from Priority 6 (Network Integration Transmission Service from Non-designated Resources) to Priority 7 (Network Integration Transmission Service from designated Network Resources) as permitted in its transmission tariff:	The Reliability Coordinator failed to comply with one (1) of the sub-components.	The Reliability Coordinator failed to comply with two (2) of the sub-components.	The Reliability Coordinator has failed to comply with three (3) of the sub-components.	The Reliability Coordinator has failed to comply with all four (4) of the sub-components.
EOP-002-3.1	R9.1.	The deficient Load-Serving Entity shall request its Reliability Coordinator to initiate an Energy Emergency Alert in accordance with Attachment 1-EOP-002 "Energy Emergency Alerts."	N/A	N/A	N/A	The Load-Serving Entity failed to request its Reliability Coordinator to initiate an Energy Emergency Alert.
EOP-002-3.1	R9.2.	The Reliability Coordinator shall submit the report to NERC for posting on the NERC Website, noting the expected total MW that may have its transmission service priority changed.	N/A	N/A	N/A	The Reliability Coordinator has failed to report to NERC as directed in the requirement.
EOP-002-3.1	R9.3.	The Reliability Coordinator shall use EEA 1 to forecast the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to Priority 7.	N/A	N/A	N/A	The Reliability Coordinator failed to use EEA 1 to forecast the change of the priority of transmission service as directed in the requirement.
EOP-002-3.1	R9.4.	The Reliability Coordinator shall use EEA 2 to announce the change of the priority of transmission service of an Interchange Transaction on the system from Priority 6 to	N/A	N/A	N/A	The Reliability Coordinator failed to use EEA 2 to announce the change

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Priority 7.				of the priority of transmission service as directed in the requirement.
EOP-003-1	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed customer load.
EOP-003-1	R2.	Each Transmission Operator and Balancing Authority shall establish plans for automatic load shedding for underfrequency or undervoltage conditions.	N/A	N/A	N/A	The responsible entity did not establish plans for automatic load shedding as directed by the requirement.
EOP-003-1	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans among other interconnected Transmission Operators and Balancing Authorities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting 5% or less of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 5% up to (and including) 10% of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 10%, up to (and including) 15% or less, of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 15% of its required entities.
EOP-003-1	R4.	A Transmission Operator or Balancing Authority shall consider one or more of these factors in designing an automatic load shedding scheme: frequency, rate of frequency decay, voltage level, rate of voltage decay, or power flow levels.	N/A	N/A	N/A	The applicable entity did not consider one of the five required elements, as directed by the requirement.
EOP-003-1	R5.	A Transmission Operator or Balancing Authority shall implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to implement load shedding in steps

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.
EOP-003-1	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed additional load after it had separated from the Interconnection when there was insufficient generating capacity to restore system frequency following automatic underfrequency load shedding.
EOP-003-1	R7.	The Transmission Operator and Balancing Authority shall coordinate automatic load shedding throughout their areas with underfrequency isolation of generating units, tripping of shunt capacitors, and other automatic actions that will occur under abnormal frequency, voltage, or power flow conditions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 5% or less of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting between 5 - 10% of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting 10-15%, inclusive, of its automatic actions.	The applicable entity did not coordinate automatic load shedding, as directed by the requirement, affecting greater than 15% of its automatic actions.
EOP-003-1	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator-controlled manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be capable of implementing the load shedding in a timeframe adequate for responding to the emergency.	N/A	The responsible entity did not have plans for operator controlled manual load shedding, as directed by the requirement.	The responsible entity has plans for manual load shedding but did not have the capability to implement the load shedding, as directed by the requirement.	The responsible entity did not have plans for operator controlled manual load shedding, as directed by the requirement nor had the capability to implement the load shedding, as directed by the requirement.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-003-2	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed customer load.
EOP-003-2	R2.	Each Transmission Operator shall establish plans for automatic load shedding for undervoltage conditions if the Transmission Operator or its associated Transmission Planner(s) or Planning Coordinator(s) determine that an under-voltage load shedding scheme is required.	N/A	N/A	N/A	The Transmission Operator did not establish plans for automatic load shedding for undervoltage conditions as directed by the requirement.
EOP-003-2	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans, excluding automatic under-frequency load shedding plans, among other interconnected Transmission Operators and Balancing Authorities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting 5% or less of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 5% up to (and including) 10% of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 10%, up to (and including) 15% or less, of its required entities.	The responsible entity did not coordinate load shedding plans, as directed by the requirement, affecting more than 15% of its required entities.
EOP-003-2	R4.	A Transmission Operator shall consider one or more of these factors in designing an automatic under voltage load shedding scheme: voltage level, rate of voltage decay, or power flow levels.	N/A	N/A	N/A	The Transmission Operator failed to consider at least one of the three elements voltage level, rate of voltage decay, or power flow levels) listed in the requirement.
EOP-003-2	R5.	A Transmission Operator or Balancing Authority shall implement load shedding, excluding automatic under-frequency load	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shedding, in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.				implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.
EOP-003-2	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority failed to shed additional load after it had separated from the Interconnection when there was insufficient generating capacity to restore system frequency following automatic underfrequency load shedding.
EOP-003-2	R7.	The Transmission Operator shall coordinate automatic undervoltage load shedding throughout their areas with tripping of shunt capacitors, and other automatic actions that will occur under abnormal voltage, or power flow conditions.	The Transmission Operator did not coordinate automatic undervoltage load shedding with 5% or less of the types of automatic actions described in the Requirement.	The Transmission Operator did not coordinate automatic undervoltage load shedding with more than 5% up to (and including) 10% of the types of automatic actions described in the Requirement.	The Transmission Operator did not coordinate automatic undervoltage load shedding with more than 10% up to (and including) 15% of the types of automatic actions described in the Requirement.	The Transmission Operator did not coordinate automatic undervoltage load shedding with more than 15% of the types of automatic actions described in the Requirement.
EOP-003-2	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator controlled manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be	N/A	The responsible entity did not have plans for operator controlled manual load shedding, as	The responsible entity has plans for manual load shedding but did not have the capability to implement the load	The responsible entity did not have plans for operator controlled manual load shedding, as directed by the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		capable of implementing the load shedding in a timeframe adequate for responding to the emergency.		directed by the requirement.	shedding, as directed by the requirement.	requirement nor had the capability to implement the load shedding, as directed by the requirement.
EOP-004-1	R1.	Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	The Regional Reliability Organization has demonstrated the existence of a regional reporting procedure, but the procedure is missing minor details or minor program/procedural elements.	The Regional Reliability Organization Regional reporting procedure have been is missing one element that would make the procedure meet the requirement.	The Regional Reliability Organization Regional has a regional reporting procedure but the procedure is not current.	The Regional Reliability Organization does not have a regional reporting procedure.
EOP-004-1	R2.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	The responsible entity failed to promptly analyze 5% or less of its disturbances on the BES.	The responsible entity failed to promptly analyze more than 5% up to (and including) 10% of its disturbances on the BES.	The responsible entity failed to promptly analyze more than 10% up to (and including) 15% of its disturbances on the BES.	The responsible entity failed to promptly analyze more than 15% of its disturbances on the BES.
EOP-004-1	R3.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	N/A	N/A	N/A	The responsible entities failed to provide a preliminary written report as directed by the requirement.
EOP-004-1	R3.1.	The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a	The responsible entity submitted the report as required in R3.1 more than 24 but less than or equal to 36 hours after the disturbance or unusual occurrence,	The responsible entity submitted the report as required in R3.1 more than 36 hours but less than or equal to 48 hours after the disturbance	The responsible entities submitted the report as required in R3.1 more than 48 hours but less than or equal to 72 hours after the disturbance or unusual	The responsible entities submitted the report as required in R3.1 more than 72-hours after the disturbance or unusual occurrence or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.	or discovery of the disturbance or unusual occurrence.	or unusual occurrence, or discovery of the disturbance or unusual occurrence.	occurrence, or discovery of the disturbance or unusual occurrence.	discovery of the disturbance or unusual occurrence.
EOP-004-1	R3.2.	Applicable reporting forms are provided in Attachments 022-1 and 022-2.	N/A	N/A	N/A	N/A
EOP-004-1	R3.3.	Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	N/A	N/A	N/A	The responsible entity did not provide its Regional Reliability Organization(s) and NERC with verbal notification or updates about a disturbance as specified in R3.3.
EOP-004-1	R3.4.	If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this	The responsible entity submitted the final report no more than 30 days past the 60 day due date; or the final report was missing one of the three elements specified in R3.4.	The responsible entity submitted the final report between 31 days and 60 days inclusive past the 60 day due date. OR The final report was missing two of the	The responsible entity submitted the final report between 61 days and 90 days inclusive past the 60 day due date	The responsible entity failed to submit the final report. OR The responsible entity submitted the final report 91 days or more past the 60 day due date

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.		three elements specified in R3.4.		OR The responsible entity submitted a final report that was missing all three of the elements specified in R3.4.
EOP-004-1	R4.	When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	N/A	N/A	N/A	The RRO did not make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.
EOP-004-1	R5.	The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.	The Regional Reliability Organization reviewed all final report recommendations less than twice a year.	The Regional Reliability Organization reviewed 75% or more final report recommendations twice a year.	The Regional Reliability Organization has not reported on any recommendation has not been acted on within two years to the NERC Planning and Operating Committees.	The Regional Reliability Organization has not reviewed the final report recommendations or did not notify the NERC Planning and Operating Committees.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-005-1	R1.	Each Transmission Operator shall have a restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system, including necessary operating instructions and procedures to cover emergency conditions, and the loss of vital telecommunications channels. Each Transmission Operator shall include the applicable elements listed in Attachment 1-EOP-005 in developing a restoration plan.	The responsible entity has a restoration plan that includes 75 % or more but less than 100% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 50% to 75% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes 25% - 50% of the applicable elements listed in Attachment 1.	The responsible entity has a restoration plan that includes less than 25% of the applicable elements listed in Attachment 1 OR the responsible entity has no restoration plan.
EOP-005-1	R2.	Each Transmission Operator shall review and update its restoration plan at least annually and whenever it makes changes in the power system network, and shall correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review or update its restoration plan when it made changes in the power system network.	The Transmission Operator failed to review and update its restoration plan at least annually.	The Transmission Operator failed to review and update its restoration plan at least annually or whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.	The Transmission Operator failed to review and update its restoration plan at least annually and whenever it made changes in the power system network, and failed to correct deficiencies found during the simulated restoration exercises.
EOP-005-1	R3.	Each Transmission Operator shall develop restoration plans with a priority of restoring the integrity of the Interconnection.	N/A	N/A	N/A	The Transmission Operator's restoration plans failed to make restoration of the integrity of the Interconnection a priority.
EOP-005-1	R4.	Each Transmission Operator shall coordinate its restoration plans with the Generator Owners and Balancing Authorities within its area, its Reliability Coordinator, and neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate its restoration plans with 5% or less of the entities identified in the requirement.	The Transmission Operator failed to coordinate its restoration plans with more than 5% up to (and including) 10% of the entities identified in the	The Transmission Operator failed to coordinate its restoration plans with more than 10% up to (and including) 15% of the entities identified in	The Transmission Operator failed to coordinate its restoration plans with more than 15% of the entities identified in the requirement.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requirement.	the requirement.	
EOP-005-1	R5.	Each Transmission Operator and Balancing Authority shall periodically test its telecommunication facilities needed to implement the restoration plan.	N/A	N/A	N/A	The responsible entity failed to periodically test its telecommunication facilities needed to implement the restoration plan.
EOP-005-1	R6.	Each Transmission Operator and Balancing Authority shall train its operating personnel in the implementation of the restoration plan. Such training shall include simulated exercises, if practicable.	The Transmission Operator or Balancing Authority failed to train 5% or less of its operating personnel in the implementation of the restoration plan.	The Transmission Operator or Balancing Authority failed to train more than 5% up to (and including) 10 % of its operating personnel in the implementation of the restoration plan.	The Transmission Operator or Balancing Authority failed to train more than 10 % up to (and including) 15% of its operating personnel in the implementation of the restoration plan.	The Transmission Operator or Balancing Authority failed to train more than 15% of its operating personnel in the implementation of the restoration plan.
EOP-005-1	R7.	Each Transmission Operator and Balancing Authority shall verify the restoration procedure by actual testing or by simulation.	N/A	N/A	N/A	The Transmission Operator or Balancing Authority did not verify the restoration procedure by actual testing or by simulation.
EOP-005-1	R8.	Each Transmission Operator shall verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan requirements for the Transmission Operator's area.	N/A	N/A	N/A	The Transmission Operator failed to verify that the number, size, availability, and location of system blackstart generating units are sufficient to meet Regional Reliability Organization restoration plan

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requirements for the Transmission Operator's area.
EOP-005-1	R9.	The Transmission Operator shall document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started and shall provide this documentation for review by the Regional Reliability Organization upon request. Such documentation may include Cranking Path diagrams.	N/A	N/A	The Transmission Operator documented the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started, but did not provide the documentation as requested by the Regional Reliability Organization.	The Transmission Operator failed to document the Cranking Paths, including initial switching requirements, between each blackstart generating unit and the unit(s) to be started.
EOP-005-1	R10.	The Transmission Operator shall demonstrate, through simulation or testing, that the blackstart generating units in its restoration plan can perform their intended functions as required in the regional restoration plan.	For less than 25% of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.	For 25% or more, but less than 50% of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.	For 50% or more, but less than 75% of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.	For 75% or more of the blackstart generating units in its restoration plan, the Transmission Operator failed to demonstrate, through simulation or testing, that these blackstart generating units can perform their intended functions as required in the regional restoration plan.
EOP-005-1	R10.1.	The Transmission Operator shall perform this simulation or testing at least once every five years.	N/A	N/A	N/A	The Transmission Operator failed to perform the required simulation or testing at least once every five years.

Complete Violation Severity Level Matrix (EOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
EOP-005-1	R11.	Following a disturbance in which one or more areas of the Bulk Electric System become isolated or blacked out, the affected Transmission Operators and Balancing Authorities shall begin immediately to return the Bulk Electric System to normal.	The responsible entity failed to comply with less than 25% of the number of sub-components.	The responsible entity failed to comply with 25% or more and less than 50% of the number of sub-components.	The responsible entity failed to comply with 50% or more and less than 75% of the number of sub-components.	The responsible entity failed to comply with more than 75% of the number of sub-components.
EOP-005-1	R11.1.	The affected Transmission Operators and Balancing Authorities shall work in conjunction with their Reliability Coordinator(s) to determine the extent and condition of the isolated area(s).	N/A	N/A	N/A	The responsible entity failed to work in conjunction with their Reliability Coordinator to determine the extent and condition of the isolated area(s)
EOP-005-1	R11.2.	The affected Transmission Operators and Balancing Authorities shall take the necessary actions to restore Bulk Electric System frequency to normal, including adjusting generation, placing additional generators on line, or load shedding.	N/A	N/A	N/A	The affected Transmission Operators and Balancing Authorities failed to take the necessary actions to restore Bulk Electric System frequency to normal.
EOP-005-1	R11.3.	The affected Balancing Authorities, working with their Reliability Coordinator(s), shall immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments as needed to facilitate the restoration. The affected Balancing Authorities shall make all attempts to maintain the adjusted Interchange Schedules, whether generation control is manual or automatic.	N/A	N/A	The responsible entity failed to make all attempts to maintain adjusted Interchange Schedules as required in R11.3	The responsible entity failed to immediately review the Interchange Schedules between those Balancing Authority Areas or fragments of those Balancing Authority Areas within the separated area and make adjustments to facilitate the restoration as required

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						in R11.3.
EOP-005-1	R11.4.	The affected Transmission Operators shall give high priority to restoration of off-site power to nuclear stations.	N/A	N/A	N/A	The affected Transmission Operators failed to give high priority to restoration of off-site power to nuclear stations.
EOP-005-1	R11.5.	The affected Transmission Operators may resynchronize the isolated area(s) with the surrounding area(s) when the following conditions are met:	N/A	N/A	N/A	The Transmission Operator attempted to resynchronize an isolated area(s) with a surrounding area(s) when one (1) or more of the sub-requirements of R11.5 were not met.
EOP-005-1	R11.5.1.	Voltage, frequency, and phase angle permit.	N/A	N/A	N/A	N/A
EOP-005-1	R11.5.2.	The size of the area being reconnected and the capacity of the transmission lines effecting the reconnection and the number of synchronizing points across the system are considered.	N/A	N/A	N/A	N/A
EOP-005-1	R11.5.3.	Reliability Coordinator(s) and adjacent areas are notified and Reliability Coordinator approval is given.	N/A	N/A	N/A	N/A
EOP-005-1	R11.5.4.	Load is shed in neighboring areas, if required, to permit successful interconnected system restoration.	N/A	N/A	N/A	N/A
EOP-006-1	R1.	Each Reliability Coordinator shall be aware of the restoration plan of each Transmission Operator in its Reliability Coordinator Area in accordance with NERC and regional requirements.	The Reliability Coordinator is not aware of 5% or less of its Transmission Operators' restoration plans.	The Reliability Coordinator is not aware of more than 5% up to (and including) 10% of its Transmission Operators'	The Reliability Coordinator is not aware of more than 10% up to (and including) 15% of its Transmission Operators' restoration	The Reliability Coordinator is not aware of more than 15% of its Transmission Operators' restoration

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				restoration plans.	plans.	plans.
EOP-006-1	R2.	The Reliability Coordinator shall monitor restoration progress and coordinate any needed assistance.	N/A	N/A	The Reliability Coordinator failed to monitor restoration progress or failed to coordinate assistance.	The Reliability Coordinator failed to monitor restoration progress and failed to coordinate assistance.
EOP-006-1	R3.	The Reliability Coordinator shall have a Reliability Coordinator Area restoration plan that provides coordination between individual Transmission Operator restoration plans and that ensures reliability is maintained during system restoration events.	N/A	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not provide coordination between less than 10% of its individual Transmission Operator restoration plans.	The Reliability Coordinator's Reliability Coordinator Area restoration plan did not provide coordination between 10% or more of the Transmission Operator restoration plans.	The Reliability Coordinator does not have a Reliability Coordinator Area restoration plan. OR The Reliability Coordinator's Reliability Coordinator Area restoration plan does not ensure reliability is maintained during system restoration events.
EOP-006-1	R4.	The Reliability Coordinator shall serve as the primary contact for disseminating information regarding restoration to neighboring Reliability Coordinators and Transmission Operators or Balancing Authorities not immediately involved in restoration.	N/A	N/A	N/A	The Reliability Coordinator failed to serve as primary contact for disseminating information regarding restoration in accordance with Requirement R4.
EOP-006-1	R5.	Reliability Coordinators shall approve, communicate, and coordinate the re-synchronizing of major system islands or synchronizing points so as not to cause a Burden on adjacent Transmission Operator, Balancing Authority, or Reliability	N/A	N/A	N/A	The Reliability Coordinator failed to approve, communicate, and coordinate the re-synchronizing of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Coordinator Areas.				major system islands or synchronizing points as stated in Requirement R5.
EOP-006-1	R6.	The Reliability Coordinator shall take actions to restore normal operations once an operating emergency has been mitigated in accordance with its restoration plan.	N/A	N/A	N/A	The Reliability Coordinator failed to take actions to restore normal operations once an operating emergency was mitigated in accordance with its restoration plan.
EOP-008-0	R1.	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have a plan to continue reliability operations in the event its control center becomes inoperable. The contingency plan must meet the following requirements:	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with one of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with two of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with three or four of the sub-requirements.	The Reliability Coordinator, Transmission Operator and Balancing Authority failed to comply with more than four of the sub-requirements.
EOP-008-0	R1.1.	The contingency plan shall not rely on data or voice communication from the primary control facility to be viable.	The responsible entity's contingency plan relies on data or voice communication from the primary control facility for up to 25% of the functions identified in R1.2 and R1.3.	The responsible entity's contingency plan relies on data or voice communication from the primary control facility for 25% to 50% of the functions identified in R1.2 and R1.3.	The responsible entity's contingency plan relies on data or voice communication from the primary control facility for 50% to 75% of the functions identified in R1.2 and R1.3.	The responsible entity's contingency plan relies on data and voice communication from the primary control facility for more than 75% of the functions identified in R1.2 and R1.3.
EOP-008-0	R1.2.	The plan shall include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing basic tie line control and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.
EOP-008-0	R1.3.	The contingency plan must address monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events. The plan shall list the critical facilities.	The responsible entity's contingency plan failed to address one of the elements listed in the requirement.	The responsible entity's contingency plan failed to address two of the elements listed in the requirement.	The responsible entity's contingency plan failed to address three of the elements listed in the requirement.	The responsible entity's contingency plan failed to address four or more of the elements listed in the requirement.
EOP-008-0	R1.4.	The plan shall include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.
EOP-008-0	R1.5.	The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.
EOP-008-0	R1.6.	The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.	N/A	N/A	N/A	The responsible entity's plan failed to include procedures and responsibilities for providing annual training to ensure that operating personnel

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						are able to implement the contingency plans.
EOP-008-0	R1.7.	The plan shall be reviewed and updated annually.	The responsible entity's plan was reviewed within 3 months of passing its annual review date.	The responsible entity's plan was reviewed within 6 months of passing its annual review date.	The responsible entity's plan was reviewed within 9 months of passing its annual review date.	The responsible entity's plan was reviewed more than 9 months of passing its annual review date.
EOP-008-0	R1.8.	Interim provisions must be included if it is expected to take more than one hour to implement the contingency plan for loss of primary control facility.	N/A	N/A	N/A	The responsible entity failed to make interim provisions when it is took more than one hour to implement the contingency plan for loss of primary control facility.
EOP-009-0	R1.	The Generator Operator of each blackstart generating unit shall test the startup and operation of each system blackstart generating unit identified in the BCP as required in the Regional BCP (Reliability Standard EOP-007-0_R1). Testing records shall include the dates of the tests, the duration of the tests, and an indication of whether the tests met Regional BCP requirements.	The Generator Operator Blackstart unit testing and recording is missing minor program/procedural elements.	Startup and testing of each Blackstart unit was performed, but the testing records are incomplete. The testing records are missing 25% or less of data requested in the requirement'.	The Generator Operator's failed to test 25% or less of the Blackstart units or testing records are incomplete. The testing records are missing between 25% and 50% of data requested in the requirement.	The Generator Operator failed to test more than 25% of its Blackstart units or does not have Blackstart testing records or is missing more than 50% of the required data.
EOP-009-0	R2.	The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.	N/A	N/A	N/A	The Generator Owner or Generator Operator did not provide the required blackstart documentation to its Regional Reliability Organization or upon request to NERC.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R1.	The Transmission Owner shall document, maintain, and publish facility connection requirements to ensure compliance with NERC Reliability Standards and applicable Regional Reliability Organization, subregional, Power Pool, and individual Transmission Owner planning criteria and facility connection requirements. The Transmission Owner's facility connection requirements shall address connection requirements for:	Not Applicable.	The Transmission Owner failed to do one of the following: Document or maintain or publish facility connection requirements as specified in the Requirement OR Failed to include one (1) of the components and specified in R1.1, R1.2 or R1.3.	The Transmission Owner failed to do one of the following: Document or maintain or publish its facility connection requirements as specified in the Requirement. OR Failed to include (2) of the components as specified in R1.1, R1.2 or R1.3 OR Failed to document or maintain or publish its facility connection requirements as specified in the Requirement **and** failed to include one (1) of the components as specified in R1.1, R1.2 or R1.3	The Transmission Owner did not develop facility connection requirements
FAC-001-0	R1.1.	Generation facilities,	N/A	N/A	N/A	N/A
FAC-001-0	R1.2.	Transmission facilities, and	N/A	N/A	N/A	N/A
FAC-001-0	R1.3.	End-user facilities	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R2.	The Transmission Owner’s facility connection requirements shall address, but are not limited to, the following items:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner’s facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	The Transmission Owner's facility connection requirements do not address one to four of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address five to eight of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner's facility connection requirements do not address nine to twelve of the sub-components. (R2.1.1 to R2.1.16)	The Transmission Owner’s facility connection requirements do not address thirteen or more of the sub-components. (R2.1.1 to R2.1.16)
FAC-001-0	R2.1.1.	Procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.2.	Procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-001-0	R2.1.3.	Voltage level and MW and MVAR capacity or demand at point of connection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.4.	Breaker duty and surge protection.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.5.	System protection and coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.6.	Metering and telecommunications.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.7.	Grounding and safety issues.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.8.	Insulation and insulation coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.9.	Voltage, Reactive Power, and power factor control.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.10.	Power quality impacts.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.11.	Equipment Ratings.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.12.	Synchronizing of facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.13.	Maintenance coordination.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.14.	Operational issues (abnormal frequency and	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		voltages).				owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.15.	Inspection requirements for existing or new facilities.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R2.1.16.	Communications and procedures during normal and emergency operating conditions.	Not Applicable.	Not Applicable.	Not Applicable.	The Transmission owner's procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems failed to include this subrequirement.
FAC-001-0	R3.	The Transmission Owner shall maintain and update its facility connection requirements as required. The Transmission Owner shall make documentation of these requirements available to the users of the transmission system, the Regional Reliability Organization, and NERC on request (five business days).	The responsible entity made the requirements available more than five business days but less than or equal to 10 business days after a request.	The responsible entity made the requirements available more than 10 business days but less than or equal to 20 business days after a request.	The responsible entity made the requirements available more than 20 business days less than or equal to 30 business days after a request.	The responsible entity made the requirements available more than 30 business days after a request.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-002-1	R1.	The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:	The Responsible Entity failed to include in their assessment one of the subrequirements.	The Responsible Entity failed to include in their assessment two of the subrequirements.	The Responsible Entity failed to include in their assessment three of the subrequirements.	The Responsible Entity failed to include in their assessment four or more of the subrequirements.
FAC-002-1	R1.1.	Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evaluation.
FAC-002-1	R1.2.	Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity’s assessment did not include the ensurance of compliance.
FAC-002-1	R1.3.	Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity’s assessment did not include the evidence of coordination.
FAC-002-1	R1.4.	Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the evidence of the studies.
FAC-002-1	R1.5.	Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly	Not Applicable.	Not Applicable.	Not Applicable.	The responsible entity's assessment did not include the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		coordinated recommendations.				documentation.
FAC-002-1	R2. (Retired)	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).	The responsible entity provided the documentation more than 30 calendar days, but not more than 45 calendar days, after a request.	The responsible entity provided the documentation more than 45 calendar days, but not more than 60 calendar days, after a request.	The responsible entity provided the documentation more than 60 calendar days, but not more than 120 calendar days, after a request.	The responsible entity provided the documentation more than 120 calendar days after a request or was unable to provide the documentation.
FAC-003-1	R1.	The Transmission owner shall prepare, and keep current, a formal transmission vegetation management program (TVMP). The TVMP shall include the Transmission Owner's objectives, practices, approved procedures, and work Specifications. 1. ANSI A300, Tree Care Operations – Tree, Shrub, and Other Woody Plant Maintenance – Standard Practices, while not a requirement of this standard, is considered to be an industry best practice.	The responsible entity did not include and keep current one of the four required elements of its TVMP, as directed by the requirement.	The responsible entity did not include and keep current two of the four required elements of its TVMP, as directed by the requirement.	The responsible entity did not include and keep current three of the four required elements of its TVMP, as directed by the requirement.	The responsible entity did not include and keep current all required elements of the TVMP, as directed by the requirement.
FAC-003-1	R1.1.	The TVMP shall define a schedule for and the type (aerial, ground) of ROW vegetation inspections. This schedule should be flexible enough to adjust for changing conditions. The inspection schedule shall be based on the anticipated growth of vegetation and any other environmental or operational factors that could impact the relationship of vegetation to the Transmission Owner's transmission lines.	N/A	N/A	The applicable entity TVMP did not define a schedule, as directed by the requirement, or the type of ROW vegetation inspections, as directed by the requirement.	The applicable entity TVMP did not define a schedule, as directed by the requirement, nor the type of ROW vegetation inspections, as directed by the requirement.
FAC-003-1	R1.2.	The Transmission Owner, in the TVMP, shall identify and document clearances between vegetation and any overhead, ungrounded supply conductors, taking into	N/A	N/A	N/A	The responsible entity, in its TVMP, failed to identify and document clearances between

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		consideration transmission line voltage, the effects of ambient temperature on conductor sag under maximum design loading, and the effects of wind velocities on conductor sway. Specifically, the Transmission Owner shall establish clearances to be achieved at the time of vegetation management work identified herein as Clearance 1, and shall also establish and maintain a set of clearances identified herein as Clearance 2 to prevent flashover between vegetation and overhead ungrounded supply conductors.				vegetation and any overhead, ungrounded supply conductors. OR The responsible entity, in its TVMP, failed to take into consideration transmission line voltage, or the effects of ambient temperature on conductor sag under maximum design loading, or the effects of wind velocities on conductor sway. OR The responsible entity, in its TVMP, failed to establish Clearance 1 or Clearance 2 values.
FAC-003-1	R1.2.1.	Clearance 1 — The Transmission Owner shall determine and document appropriate clearance distances to be achieved at the time of transmission vegetation management work based upon local conditions and the expected time frame in which the Transmission Owner plans to return for future vegetation management work. Local conditions may include, but are not limited to: operating voltage, appropriate vegetation management techniques, fire risk, reasonably anticipated tree and conductor movement, species types and growth rates, species failure characteristics, local climate and rainfall patterns, line terrain and elevation, location	N/A	N/A	N/A	The responsible entity failed to determine and document an appropriate clearance distance to be achieved at the time of transmission vegetation management work taking into account local conditions and the expected time frame in which the responsible entity expects to return for future vegetation

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		of the vegetation within the span, and worker approach distance requirements. Clearance 1 distances shall be greater than those defined by Clearance 2 below.				management work. OR The responsible entity documented a Clearance 1 value that was smaller than its Clearance 2 value.
FAC-003-1	R1.2.2.	Clearance 2 — The Transmission Owner shall determine and document specific radial clearances to be maintained between vegetation and conductors under all rated electrical operating conditions. These minimum clearance distances are necessary to prevent flashover between vegetation and conductors and will vary due to such factors as altitude and operating voltage. These Transmission Owner-specific minimum clearance distances shall be no less than those set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard 516-2003 (*Guide for Maintenance Methods on Energized Power Lines*) and as specified in its Section 4.2.2.3, Minimum Air Insulation Distances without Tools in the Air Gap.	N/A	N/A	N/A	The responsible entity failed to determine and document Clearance 2 values taking into account local conditions and the expected time frame in which the responsible entity expects to return for future vegetation management work.
FAC-003-1	R1.2.2.1.	Where transmission system transient overvoltage factors are not known, clearances shall be derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.	N/A	N/A	N/A	Where transmission system transient overvoltage factors were not known, clearances were not derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-003-1	R1.2.2.2.	Where transmission system transient overvoltage factors are known, clearances shall be derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.	Not Applicable.	Not Applicable.	Not Applicable.	Where transmission system transient overvoltage factors are known, clearances were not derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.
FAC-003-1	R1.3.	All personnel directly involved in the design and implementation of the TVMP shall hold appropriate qualifications and training, as defined by the Transmission Owner, to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, one of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, 5% or less of those persons did not hold appropriate qualifications and training to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, two of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, more than 5% up to (and including) 10%of those persons did not hold appropriate qualifications and training to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, three of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, more than 10% up to (and including) 15%of those persons did not hold appropriate qualifications and training to perform their duties.	For responsible entities directly involving fewer than 20 persons in the design and implementation of the TVMP, more than three of those persons did not hold appropriate qualifications and training to perform their duties. For responsible entities directly involving 20 or more persons in the design and implementation of the TVMP, more than 15% of those persons did not hold appropriate qualifications and training to perform their duties.

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
FAC-003-1	R1.4.	Each Transmission Owner shall develop mitigation measures to achieve sufficient clearances for the protection of the transmission facilities when it identifies locations on the ROW where the Transmission Owner is restricted from attaining the clearances specified in Requirement 1.2.1.	N/A	N/A	N/A	The responsible entity's TVMP does not include mitigation measures to achieve sufficient clearances where restrictions to the ROW are in effect.
FAC-003-1	R1.5.	Each Transmission Owner shall establish and document a process for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage. This is so that action (temporary reduction in line rating, switching line out of service, etc.) may be taken until the threat is relieved.	N/A	N/A	N/A	The responsible entity did not establish or did not document a process for the immediate communication of vegetation conditions that present an imminent threat of line outage, as directed by the requirement.
FAC-003-1	R2.	The Transmission Owner shall create and implement an annual plan for vegetation management work to ensure the reliability of the system. The plan shall describe the methods used, such as manual clearing, mechanical clearing, herbicide treatment, or other actions. The plan should be flexible enough to adjust to changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors that may have an impact on the reliability of the transmission systems. Adjustments to the plan shall be documented as they occur. The plan should take into consideration the time required to obtain permissions or permits from landowners or regulatory authorities. Each Transmission Owner shall have systems and procedures for documenting and tracking	The responsible entity did not meet one of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the	The responsible entity did not meet two of the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan)	The responsible entity did not meet the three required elements (including in the annual plan a description of methods used for vegetation management, maintaining documentation of adjustments to the annual plan, or having systems and procedures for tracking work performed as part of the annual plan) specified in the requirement.	The responsible entity does not have an annual plan for vegetation management. OR The responsible entity has not implemented the annual plan for vegetation management.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the planned vegetation management work and ensuring that the vegetation management work was completed according to work specifications.	requirement.	specified in the requirement.		
FAC-003-1	R3.	The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.	The responsible entity failed to provide a quarterly outage report, but did not experience any reportable outages. OR The responsible entity provided a quarterly report, but failed to report in the manner specified by one or more of the following subcomponents of R3: R3.1 or R3.2.	The responsible entity provided a quarterly report, but failed to include information required by R3.3.	The responsible entity provided a quarterly outage report, but failed to include a reportable Category 3 outage as described in R3.4.3.	The responsible entity experienced reportable outages but failed to provide a quarterly report. OR The responsible entity provided a quarterly outage report, but failed to include a reportable Category 1 (as described in R3.4.1) or Category 2 outage (as described in R3.4.2).
FAC-003-1	R3.1.	Multiple sustained outages on an individual line, if caused by the same vegetation, shall be reported as one outage regardless of the actual number of outages within a 24-hour period.	N/A	N/A	N/A	N/A
FAC-003-1	R3.2.	The Transmission Owner is not required to report to the RRO, or the RRO's designee, certain sustained transmission line outages caused by vegetation: (1) Vegetation-related outages that result from vegetation falling into lines from outside the ROW that result from natural disasters shall not be considered reportable (examples of disasters that could create non-reportable outages include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, major storms as defined either by the Transmission Owner or an applicable	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		regulatory body, ice storms, and floods), and (2) Vegetation-related outages due to human or animal activity shall not be considered reportable (examples of human or animal activity that could cause a non-reportable outage include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural activities or horticultural or agricultural activities, or removal or digging of vegetation).				
FAC-003-1	R3.3.	The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, shall include at a minimum: the name of the circuit(s) outaged, the date, time and duration of the outage; a description of the cause of the outage; other pertinent comments; and any countermeasures taken by the Transmission Owner.	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.	An outage shall be categorized as one of the following:	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.1.	Category 1 — Grow-ins: Outages caused by vegetation growing into lines from vegetation inside and/or outside of the ROW;	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.2.	Category 2 — Fall-ins: Outages caused by vegetation falling into lines from inside the ROW;	N/A	N/A	N/A	N/A
FAC-003-1	R3.4.3.	Category 3 — Fall-ins: Outages caused by vegetation falling into lines from outside the ROW.	N/A	N/A	N/A	N/A
FAC-003-1	R4.	The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions	Not applicable.	Not applicable.	The RRO did not submit a quarterly report to NERC for a	The RRO did not submit a quarterly report to NERC for more than two

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		taken by the RRO as a result of any of the reported outages.			single quarter.	consecutive quarters.
FAC-008-1	R1.	The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:	The responsible entity failed to include in their methodology one of the subcomponents of R1.3, (R1.3.1 to R1.3.5).	The responsible entity failed to include in their methodology two of the subcomponents of R1.3, (R1.3.1 to R1.3.5).	The responsible entity rating methodology did not address either of the sub-components of R1.2 (R1.2.1 or R1.2.2). OR The responsible entity failed to include in their methodology three of the subcomponents of R1.3, (R1.3.1 to R1.3.5).	The Transmission Owner or Generation Owner does not have a documented Facility Ratings Methodology for use in developing facility ratings. The responsible entity's rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in R1.1. OR The responsible entity rating methodology did not address the components of R1.2, (R1.2.1 and R1.2.2). OR The responsible entity failed to include in their methodology four or more of the subcomponents of R1.3, (R1.3.1 to R1.3.5).
FAC-008-1	R1.1.	A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.	N/A	N/A	N/A	N/A
FAC-008-1	R1.2.	The method by which the Rating (of major BES equipment that comprises a Facility) is	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		determined.				
FAC-008-1	R1.2.1.	The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.	N/A	N/A	N/A	N/A
FAC-008-1	R1.2.2.	The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.	Consideration of the following:	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.1.	Ratings provided by equipment manufacturers.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.2.	Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.3.	Ambient conditions.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.4.	Operating limitations.	N/A	N/A	N/A	N/A
FAC-008-1	R1.3.5.	Other assumptions.	N/A	N/A	N/A	N/A
FAC-008-1	R2. (Retired)	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.	The responsible entity made the Facility Ratings Methodology available within more than 15 business days but less than or equal to 25 business days after a request.	The responsible entity made the Facility Ratings Methodology available within more than 25 business days but less than or equal to 35 business days after a request.	The responsible entity made the Facility Ratings Methodology available within more than 35 business days but less than or equal to 45 business days after a request.	The responsible entity failed to make available the Facility Ratings Methodology available in more than 45 business days after a request.
FAC-008-1	R3. (Retired)	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a	The responsible entity provided a response in more than 45 calendar days but less than or	The responsible entity provided a response in more than 60 calendar	The responsible entity provided a response in more than 70 calendar days but less than or	The responsible entity failed to provide a response as required in more than 80 calendar

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.	equal to 60 calendar days after a request.	days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings Methodology but did not indicate why no change will be made.	equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings Methodology.	days after a request.
FAC-008-3	R1.	Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. [See standard for documentation requirements]	N/A	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
FAC-008-3	R2.	Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. [See standard for methodology	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1.	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		requirements]	• 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	• 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
FAC-008-3	R3.	Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: [See standard for methodology requirements]	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2 OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					• 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	• 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
FAC-008-3	R4. (Retired)	Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.	The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.	The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)
FAC-008-3	R5. (Retired)	If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.	The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)	The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility	The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation.	The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)	(R5)	
FAC-008-3	R6.	Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
FAC-008-3	R7.	Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requesting entities.
FAC-008-3	R8.	Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): [See standard for requirements of providing requested information]	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			requesting entity. (R8, Part 8.2)	entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	required Rating information to the requesting entity. (R8, Part 8.2)	Rating information to the requesting entity. (R8, Part 8.1)
FAC-009-1	R1.	The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for 5% or less of its solely owned and jointly owned Facilities.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for more than 5% up to (and including) 10% of its solely owned and jointly owned Facilities.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities.	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings Methodology for more than 15% of its solely owned and jointly owned Facilities.
FAC-009-1	R2.	The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to 15 calendar days.	The Transmission Owner or Generator Owner provided its Facility Ratings to all but one of the requesting entities.	The Transmission Owner or Generator Owner provided its Facility Ratings to two of the requesting entities.	The Transmission Owner or Generator Owner has provided its Facility Ratings to none of the requesting entities within 30 calendar days of the associated schedules.
FAC-010-2.1	R1	The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				address R1.2		OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
FAC-010-2.1	R2.	The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 – R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
FAC-010-2.1	R3.	The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			through R3.6.	through R3.6.		R3.1 through R3.6.
FAC-010-2.1	R4.	The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:	One or both of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	One of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of	One of the following: The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and	One of the following: The Planning Authority failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				the change.	changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
FAC-010-2.1	R5. (Retired)	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority	The Planning Authority received documented technical	The Planning Authority received documented	The Planning Authority received documented technical comments on	The Planning Authority received documented technical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.
FAC-011-2	R1.	The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
FAC-011-2	R2.	The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance	The Reliability Coordinator's SOL Methodology	Not applicable.	The Reliability Coordinator's SOL Methodology	The Reliability Coordinator's SOL Methodology

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		consistent with the following:	requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)		requires that SOLs are set to meet BES performance in the precontingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
FAC-011-2	R3.	The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
FAC-011-2	R4	The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:	One or both of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed	One of the following : The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Complete Violation Severity Level Matrix (FAC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days after the effectiveness of the change.	methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						methodology was provided up to 30 calendar days after the effectiveness of the change.
FAC-011-2	R5. (Retired)	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.
FAC-013-1	R1.	The Reliability Coordinator and Planning Authority shall each establish a set of inter-regional and intra-regional Transfer Capabilities that is consistent with its current Transfer Capability Methodology.	The responsible entity has established a set of Transfer Capabilities, but 5% or less of all Transfer Capabilities required to be established, are inconsistent with the current Transfer Capability	The responsible entity has established a set of Transfer Capabilities, but more than 5% up to (and including) 10% of all Transfer Capabilities required to be established,	The responsible entity has established a set of Transfer Capabilities, but more than 10% up to (and including) 15% of all Transfer Capabilities required to be established, are inconsistent with the current Transfer	The responsible entity has established a set of Transfer Capabilities, but more than 15% of those Transfer Capabilities are not consistent with the current Transfer Capability Methodology

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Methodology.	are inconsistent with the current Transfer Capability Methodology.	Capability Methodology.	OR The responsible entity has not established a set of Transfer Capabilities.
FAC-013-1	R2.	The Reliability Coordinator and Planning Authority shall each provide its inter-regional and intra-regional Transfer Capabilities to those entities that have a reliability-related need for such Transfer Capabilities and make a written request that includes a schedule for delivery of such Transfer Capabilities as follows:	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting one schedule by up to 15 calendar days.	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting two schedules.	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting more than two schedules.	The Reliability Coordinator or Planning Authority has provided its Transfer Capabilities but missed meeting all schedules within 30 calendar days of the associated schedules.
FAC-013-1	R2.1.	The Reliability Coordinator shall provide its Transfer Capabilities to its associated Regional Reliability Organization(s), to its adjacent Reliability Coordinators, and to the Transmission Operators, Transmission Service Providers and Planning Authorities that work in its Reliability Coordinator Area.	The responsible entity failed to provide Transfer Capabilities to 5% or less of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 5% up to (and including) 10% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 10% up to (and including) 15% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 15% of the required entities.
FAC-013-1	R2.2.	The Planning Authority shall provide its Transfer Capabilities to its associated Reliability Coordinator(s) and Regional Reliability Organization(s), and to the Transmission Planners and Transmission Service Provider(s) that work in its Planning Authority Area.	The responsible entity failed to provide Transfer Capabilities 5% or less of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 5% up to (and including) 10% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 10% up to (and including) 15% of the required entities.	The responsible entity failed to provide Transfer Capabilities to more than 15% of the required entities.
FAC-013-2	R1.	Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology:	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		information: [See standard pdf for requirements of the Transfer Capability methodology]		into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	• Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.
FAC-013-2	R2.	Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: [See standard pdf for requirements of issuing the Transfer Capability Methodology]	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	90 calendar days but not more than 120 calendar days after receipt of a request.	methodology more than 120 calendar days after receipt of a request.
FAC-013-2	R3. (Retired)	If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.
FAC-013-2	R4.	During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days,	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Planning Horizon.	calendar days.	more than 30 calendar days, but not by more than 60 calendar days.	but not by more than 90 calendar days.	calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.
FAC-013-2	R5.	Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
FAC-013-2	R6.	If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days	The Planning Coordinator provided the requested data as required in Requirement R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information.	after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.
FAC-014-2	R1.	The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.	There are SOLs, for the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs, for the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)	There are SOLs for the Reliability Coordinator Area, but 75% or more of these the SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R1)
FAC-014-2	R2.	The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but from 1% up to but less than 25% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)	The Transmission Operator has established SOLs for its portion of the Reliability Coordinator Area, but 75% or more of these SOLs are inconsistent with the Reliability Coordinator's SOL Methodology. (R2)
FAC-014-2	R3.	The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology.	There are SOLs, for the Planning Coordinator Area, but from 1% up to, but less than, 25% of these	There are SOLs, for the Planning Coordinator Area, but 25% or more, but less than 50% of	There are SOLs for the Planning Coordinator Area, but 50% or more, but less than 75% of these SOLs are	There are SOLs, for the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R3)	inconsistent with the Planning Coordinator's SOL Methodology. (R3)	with the Planning Coordinator's SOL Methodology. (R3)
FAC-014-2	R4.	The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology.	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but up to 25% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 25% or more, but less than 50% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Reliability Coordinator Area, but 50% or more, but less than 75% of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)	The Transmission Planner has established SOLs for its portion of the Planning Coordinator Area, but 75% or more of these SOLs are inconsistent with the Planning Coordinator's SOL Methodology. (R4)
FAC-014-2	R5.	The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows:	The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all the requesting entities but missed meeting one or more of the schedules by less than 15 calendar days. (R5)	One of the following: The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all but one of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the	One of the following: The responsible entity provided its SOLs (including the subset of SOLs that are IROLs) to all but two of the requesting entities within the schedules provided. (R5) Or The responsible entity provided its SOLs to all the requesting entities but missed meeting one or more of the schedules for 30	One of the following: The responsible entity failed to provide its SOLs (including the subset of SOLs that are IROLs) to more than two of the requesting entities within 45 calendar days of the associated schedules. (R5) OR The supporting information provided with the IROLs does not address 5.1.1 and 5.1.2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				schedules for 15 or more but less than 30 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.4	or more but less than 45 calendar days. (R5) OR The supporting information provided with the IROLs does not address 5.1.3	
FAC-014-2	R6.	The Planning Authority shall identify the subset of multiple contingencies (if any), from Reliability Standard TPL-003 which result in stability limits.	The Planning Authority failed to notify the Reliability Coordinator in accordance with R6.2	Not applicable.	The Planning Authority identified the subset of multiple contingencies which result in stability limits **but** did not provide the list of multiple contingencies and associated limits to one Reliability Coordinator that monitors the Facilities associated with these limits. (R6.1)	The Planning Authority did not identify the subset of multiple contingencies which result in stability limits. (R6) OR The Planning Authority identified the subset of multiple contingencies which result in stability limits **but** did not provide the list of multiple contingencies and associated limits to more than one Reliability Coordinator that monitors the Facilities associated with these limits. (R6.1)
FAC-501-WECC-1	R1.	Transmission Owners shall have a TMIP detailing their inspection and maintenance	The TMIP does not include associated	The TMIP does not include associated	The TMIP does not include associated	The TMIP does not include associated

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		requirements that apply to all transmission facilities necessary for System Operating Limits associated with each of the transmission paths identified in table titled "Major WECC Transfer Paths in the Bulk Electric System."	Facilities for one of the Paths identified in Attachment 1 FAC-501-WECC-1 as required by R.1 but Transmission Owners are performing maintenance and inspection for the missing Facilities.	Facilities for two of the Paths identified in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" as required by R.1 and Transmission Owners are not performing maintenance and inspection for the missing Facilities.	Facilities for three of the Paths identified in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" as required by R.1 and Transmission Owners are not performing maintenance and inspection for the missing Facilities.	Facilities for more than three of the Paths identified in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" as required by R.1 and Transmission Owners are not performing maintenance and inspection for the missing Facilities.
FAC-501-WECC-1	R1.1.	Transmission Owners shall annually review their TMIP and update as required.	Transmission Owners did not review their TMIP annually as required by R.1.1.	N/A	N/A	N/A
FAC-501-WECC-1	R2.	Transmission Owners shall include the maintenance categories in Attachment 1-FAC-501-WECC-1 when developing their TMIP.	The TMIP does not include one maintenance category identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.	The TMIP does not include two maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.	The TMIP does not include three maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.	The TMIP does not exist or does not include more than three maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required by R.2 but Transmission Owners are performing maintenance and inspection for the missing maintenance categories.
FAC-501-WECC-1	R3.	Transmission Owners shall implement and follow their TMIP.	Transmission Owners do not have maintenance and inspection records as	Transmission Owners are not performing maintenance and	Transmission Owners are not performing maintenance and inspection for two	Transmission Owners are not performing maintenance and inspection for more

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by R.3 but have evidence that they are implementing and following their TMIP.	inspection for one maintenance category identified in Attachment 1 FAC-501-WECC-1 as required in R3.	maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required in R3.	than two maintenance categories identified in Attachment 1 FAC-501-WECC-1 as required in R3.

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-001-3	R1.	The Load-Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for:	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for: (see below)
INT-001-3	R1.1.	All Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.	The Load-Serving, Purchasing-Selling Entity experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for all Dynamic Schedules at the expected average MW profile for each hour.
INT-001-3	R2.	The Sink Balancing Authority shall ensure that Arranged Interchange is submitted to the Interchange Authority:	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority (see below)

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-001-3	R2.1.	If a Purchasing-Selling Entity is not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority if a Purchasing-Selling Entity was not involved in the Interchange, such as delivery from a jointly owned generator.
INT-001-3	R2.2.	For each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced one instance of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced two instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced three instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.	The Sink Balancing Authority experienced four instances of failing to ensure that Arranged Interchange was submitted to the Interchange Authority for each bilateral Inadvertent Interchange payback.
INT-003-3	R1.	Each Receiving Balancing Authority shall confirm Interchange Schedules with the Sending Balancing Authority prior to implementation in the Balancing Authority's ACE equation.	There shall be a separate Lower VSL, if either of the following conditions exists: One instance of entering a schedule into its ACE equation without confirming the	There shall be a separate Moderate VSL, if either of the following conditions exists: Two instances of entering a schedule into its ACE equation	There shall be a separate High VSL, if either of the following conditions exists: Three instances of entering a schedule into its ACE equation without confirming the schedule	There shall be a separate Severe VSL, if either of the following conditions exists: Four or more instances of entering a schedule into its ACE equation without

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. One instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Two instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	as specified in R1, R1.1, R1.1.1 and R1.1.2. Three instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2. Four or more instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-003-3	R1.1.	The Sending Balancing Authority and Receiving Balancing Authority shall agree on Interchange as received from the Interchange Authority, including:	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-3	R1.1.1.	Interchange Schedule start and end time.	The Balancing Authority experienced one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	The Balancing Authority experienced four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-3	R1.1.2	Energy profile.	The Balancing Authority experienced	The Balancing Authority	The Balancing Authority experienced	The Balancing Authority experienced

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			one instance of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	experienced two instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	three instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.	four instances of entering a schedule into its ACE equation without confirming the schedule as specified in R1, R1.1, R1.1.1 and R1.1.2.
INT-003-3	R1.2.	If a high voltage direct current (HVDC) tie is on the Scheduling Path, then the Sending Balancing Authorities and Receiving Balancing Authorities shall coordinate the Interchange Schedule with the Transmission Operator of the HVDC tie.	The sending or receiving Balancing Authority experienced one instance of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced two instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced three instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2	The sending or receiving Balancing Authority experienced four instances of not coordinating the Interchange Schedule with the Transmission Operator of the HVDC tie as specified in R1.2
INT-004-2	R1.	At such time as the reliability event allows for the reloading of the transaction, the entity that initiated the curtailment shall release the limit on the Interchange Transaction tag to allow reloading the transaction and shall communicate the release of the limit to the Sink Balancing Authority.	The entity that initiated the curtailment failed to communicate the transaction reload to the Sink Balancing Authority	The entity that initiated the curtailment failed to reload the transaction and failed to communicate to the Sink Balancing Authority	N/A	N/A
INT-004-2	R2.	The Purchasing-Selling Entity responsible for tagging a Dynamic Interchange Schedule shall ensure the tag is updated for the next available scheduling hour and future hours when any one of the following occurs:	N/A	N/A	The responsible entity failed to update the tag when required by sub-requirements R2.1 or R2.2.	The responsible entity failed to update the tag when required by sub-requirement R2.3.
INT-004-2	R2.1.	The average energy profile in an hour is greater than 250 MW and in that hour the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +10%.				
INT-004-2	R2.2.	The average energy profile in an hour is less than or equal to 250 MW and in that hour the actual hourly integrated energy deviates from the hourly average energy profile indicated on the tag by more than +25 megawatt-hours.	N/A	N/A	N/A	N/A
INT-004-2	R2.3.	A Reliability Coordinator or Transmission Operator determines the deviation, regardless of magnitude, to be a reliability concern and notifies the Purchasing-Selling Entity of that determination and the reasons.	N/A	N/A	N/A	N/A
INT-005-3	R1.	Prior to the expiration of the time period defined in the timing requirements tables in this standard, Column A, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment to all reliability entities involved in the Interchange.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities
INT-005-3	R1.1.	When a Balancing Authority or Reliability Coordinator initiates a Curtailment to Confirmed or Implemented Interchange for reliability, the Interchange Authority shall distribute the Arranged Interchange information for reliability assessment only to the Source Balancing Authority and the Sink Balancing Authority.	N/A	N/A	The Responsible Entity initiated a Curtailment to Confirmed or Implemented Interchange for reliability but the Interchange Authority failed to distribute the Arranged Interchange information to the Source Balancing Authority or the Sink Balancing Authority.	The Responsible Entity initiated a Curtailment to Confirmed or Implemented Interchange for reliability but the Interchange Authority failed to distribute the Arranged Interchange information to the Source Balancing Authority and the Sink Balancing Authority.
INT-006-3	R1.	Prior to the expiration of the reliability	The Responsible	The Responsible	The Responsible Entity	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		assessment period defined in the timing requirements tables in this standard, Column B, the Balancing Authority and Transmission Service Provider shall respond to each On-time Request for Interchange (RFI), and to each Emergency RFI and Reliability Adjustment RFI from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange	Entity failed on one occasion to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	Entity failed on two occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	failed on three occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.	Entity failed on four occasions to respond to a request from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange.
INT-006-3	R1.1.	Each involved Balancing Authority shall evaluate the Arranged Interchange with respect to:	The Balancing Authority failed to evaluate arranged interchange with respect to one of the requirements in the 3 sub-components.	N/A	The Balancing Authority failed to evaluate arranged interchange with respect to two of the requirements in the 3 sub-components.	The Balancing Authority failed to evaluate arranged interchange with respect to three of the requirements in the 3 sub-components.
INT-006-3	R1.1.1.	Energy profile (ability to support the magnitude of the Interchange).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Energy profile (ability to support the magnitude of the Interchange).
INT-006-3	R1.1.2.	Ramp (ability of generation maneuverability to accommodate).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Ramp (ability of generation maneuverability to accommodate).
INT-006-3	R1.1.3.	Scheduling path (proper connectivity of Adjacent Balancing Authorities).	N/A	N/A	N/A	The Balancing Authority failed to evaluate Scheduling path (proper connectivity of Adjacent Balancing Authorities).

Complete Violation Severity Level Matrix (INT)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
INT-006-3	R1.2.	Each involved Transmission Service Provider shall confirm that the transmission service arrangements associated with the Arranged Interchange have adjacent Transmission Service Provider connectivity, are valid and prevailing transmission system limits will not be violated	The Transmission Service Provider experienced one instance of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced two instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experienced three instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.	The Transmission Service Provider experience four instances of failing to confirm that the transmission service arrangements associated with the Arranged Interchange had adjacent Transmission Service Provider connectivity, were valid and prevailing transmission system limits would not be violated.
INT-007-1	R1.	The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:	The Interchange Authority failed to verify one time, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)	The Interchange Authority failed to verify two times, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)	The Interchange Authority failed to verify three times, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)	The Interchange Authority failed to verify four times, as indicated in R1.1, ~~R1.2,~~ R1.3, R1.3.1, R1.3.2, R1.3.3, or R1.3.4 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange. (R1.2 retired)
INT-007-1	R1.1.	Source Balancing Authority megawatts equal sink Balancing Authority megawatts	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to	The Interchange Authority failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(adjusted for losses, if appropriate).	verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.2. (Retired)	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.	The following are defined:	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.1.	Generation source and load sink.	The Interchange Authority failed to verify one time, as	The Interchange Authority failed to verify two times, as	The Interchange Authority failed to verify three times, as	The Interchange Authority failed to verify four times, as

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.2.	Megawatt profile.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.3.	Ramp start and stop times.	The Interchange Authority failed to verify one time, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify two times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify three times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	The Interchange Authority failed to verify four times, as indicated in R1 that Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.3.4.	Interchange duration.	The Interchange Authority failed to verify one time, as indicated in R1 that	The Interchange Authority failed to verify two times, as indicated in R1 that	The Interchange Authority failed to verify three times, as indicated in R1 that	The Interchange Authority failed to verify four times, as indicated in R1 that

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.	Arranged Interchange was balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange.
INT-007-1	R1.4.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with minor exception and is substantially compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval, with some exception and is mostly compliant with the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval but was substantially deficient in meeting the directives of the requirement.	Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment did not provided approval and failed to meet the requirement.
INT-008-3	R1.	Prior to the expiration of the time period defined in the Timing Table, Column C, the Interchange Authority shall distribute to all Balancing Authorities (including Balancing Authorities on both sides of a direct current tie), Transmission Service Providers and Purchasing-Selling Entities involved in the Arranged Interchange whether or not the Arranged Interchange has transitioned to a Confirmed Interchange.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as deliniated in R1.1, R1.1.1 or R1.1.2.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities or no evidence provided.
INT-008-3	R1.1.	For Confirmed Interchange, the Interchange	The Interchange	The Interchange	The Interchange	The Interchange

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Authority shall also communicate:	Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-3	R1.1.1.	Start and stop times, ramps, and megawatt profile to Balancing Authorities.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-008-3	R1.1.2.	Necessary Interchange information to NERC-identified reliability analysis services.	The Interchange Authority experienced one occurrence of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced two occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced three occurrences of not distributing information to all involved reliability entities as defined in R1.	The Interchange Authority experienced four occurrences of not distributing information to all involved reliability entities as defined in R1 or no evidence provided.
INT-009-1	R1.	The Balancing Authority shall implement Confirmed Interchange as received from the Interchange Authority.	N/A	N/A	N/A	The responsible entity failed to implement a Confirmed Interchange as received from the Interchange Authority.
INT-010-1	R1.	The Balancing Authority that experiences a loss of resources covered by an energy sharing agreement shall ensure that a request for an Arranged Interchange is submitted with a start time no more than 60 minutes	The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an	The responsible entity that experienced a loss of resources that exceeded 60	The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an	The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		beyond the resource loss. If the use of the energy sharing agreement does not exceed 60 minutes from the time of the resource loss, no request for Arranged Interchange is required.	energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was more than 60 minutes but less than 75 minutes beyond the resource loss.	minutes and was covered by an energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was 75 minutes or more, but less than 90 minutes beyond the resource loss.	energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was 90 minutes or more, but less than 105 minutes beyond the resource loss.	energy sharing agreement ensured that a request for an Arranged Interchange was submitted, but with a start time that was more than 105 minutes beyond the resource loss. OR The responsible entity that experienced a loss of resources that exceeded 60 minutes and was covered by an energy sharing agreement, failed to ensure that a request for an Arranged Interchange was submitted.
INT-010-1	R2.	For a modification to an existing Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit the modified Arranged Interchange reflecting that modification within 60 minutes of the initiation of the event.	N/A	N/A	N/A	The responsible entity failed to direct a Balancing Authority to submit the modified Arranged Interchange reflecting the modification, within 60 minutes of the initiation of the event.
INT-010-1	R3.	For a new Interchange schedule that is directed by a Reliability Coordinator for current or imminent reliability-related reasons, the Reliability Coordinator shall direct a Balancing Authority to submit an Arranged Interchange reflecting that Interchange schedule within 60 minutes of	N/A	N/A	N/A	The responsible entity failed to direct a Balancing Authority to submit an Arranged Interchange reflecting the new Interchange schedule within 60

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the initiation of the event.				minutes of the initiation of the event.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-001-1.1	R1.	Each Regional Reliability Organization, subregion, or interregional coordinating group shall establish one or more Reliability Coordinators to continuously assess transmission reliability and coordinate emergency operations among the operating entities within the region and across the regional boundaries.	The RRO, subregion or interregional coordinating group did not communicate the assignment of the Reliability Coordinators to operating entities clearly.	The RRO, subregion or interregional coordinating group did not clearly identify the coordination of Reliability Coordinator areas within the region.	The RRO, subregion or interregional coordinating group did not coordinate assignment of the Reliability Coordinators across regional boundaries.	The RRO, subregion or interregional coordinating group did not assign any Reliability Coordinators.
IRO-001-1.1	R2.	The Reliability Coordinator shall comply with a regional reliability plan approved by the NERC Operating Committee.	The Reliability Coordinator has failed to follow the administrative portions of its regional reliability plan.	The Reliability Coordinator has failed to follow steps in its regional reliability plan that requires operator interventions or actions.	The Reliability Coordinator does not have a regional reliability plan approved by the NERC OC.	The Reliability Coordinator does not have an unapproved regional reliability plan.
IRO-001-1.1	R3.	The Reliability Coordinator shall have clear decision-making authority to act and to direct actions to be taken by Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities within its Reliability Coordinator Area to preserve the integrity and reliability of the Bulk Electric System. These actions shall be taken without delay, but no longer than 30 minutes.	N/A	N/A	The Reliability Coordinator cannot demonstrate that it has clear authority to act or direct actions to preserve transmission security and reliability of the Bulk Electric System.	The Reliability Coordinator failed to take or direct to preserve the reliability and security of the Bulk Electric System within 30 minutes of identifying those actions.
IRO-001-1.1	R4.	Reliability Coordinators that delegate tasks to other entities shall have formal operating agreements with each entity to which tasks are delegated. The Reliability Coordinator shall verify that all delegated tasks are understood, communicated, and addressed within its Reliability Coordinator Area. All	1. Less than 25% of the tasks are not documented in the agreement or 2. Less than 25% of the tasks are not performed according	1. More than 25% but 50% or less of the tasks are not documented in the agreement or 2. More than 25% but 50% or less of	1. More than 50% but 75% or less of the tasks are not documented in the agreement or 2. More than 50% but 75% or less of the tasks are not performed	1. There is no formal operating agreement for tasks delegated by the Reliability Coordinator, 2. More than 75% of the tasks are not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		responsibilities for complying with NERC and regional standards applicable to Reliability Coordinators shall remain with the Reliability Coordinator.	to the agreement.	the tasks are not performed according to the agreement.	according to the agreement.	documented in the agreement or 3. More than 75% of the tasks are not performed according to the agreement.
IRO-001-1.1	R5.	The Reliability Coordinator shall list within its reliability plan all entities to which the Reliability Coordinator has delegated required tasks.	5% or less of the delegate entities are not identified in the reliability plan.	More than 5% up to (and including) 10% of the delegate entities are not identified in the reliability plan.	More than 10% up to (and including) 15% of the delegate entities are not identified in the reliability plan.	There is no reliability plan. OR More than 15% of the delegate entities are not identified in the reliability plan.
IRO-001-1.1	R6.	The Reliability Coordinator shall verify that all delegated tasks are carried out by NERC-certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that 5% or less of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that more than 5% up to (and including) 10% of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that more than 10% up to (and including) 15% of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.	The Reliability Coordinator failed to demonstrate that more than 15% of its delegated tasks were being performed by NERC certified Reliability Coordinator operating personnel.
IRO-001-1.1	R7.	The Reliability Coordinator shall have clear, comprehensive coordination agreements with adjacent Reliability Coordinators to ensure that System Operating Limit or Interconnection Reliability Operating Limit violation mitigation requiring actions in adjacent Reliability Coordinator Areas are coordinated.	The Reliability Coordinator has demonstrated the existence of coordination agreements with adjacent Reliability Coordinators but the agreements are not clear or comprehensive.	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to	The Reliability Coordinator has demonstrated the existence of the coordination agreements with adjacent Reliability Coordinators but the agreements do not coordinate actions required in the adjacent Reliability Coordinator to mitigate SOL and	The Reliability Coordinator has failed to demonstrate the existence of any coordination agreements with adjacent Reliability Coordinators.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigate SOL or IROL violations in its own Reliability Coordinator area.	IROL violations in its own Reliability Coordinator area.	
IRO-001-1.1	R8.	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.	N/A	The responsible entity could not comply with a directive due to qualified reasons (violation of safety, equipment or regulatory or statutory requirements) and did not immediately inform the Reliability Coordinator.	N/A	The responsible entity did not follow the Reliability Coordinator's directive.
IRO-001-1.1	R9.	The Reliability Coordinator shall act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of any other entity.	N/A	N/A	N/A	The Reliability Coordinator did not act in the interests of reliability for the overall Reliability Coordinator Area and the Interconnection before the interests of one or more other entities.
IRO-003-2	R1.	Each Reliability Coordinator shall monitor all Bulk Electric System facilities, which may include sub-transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time,	N/A	N/A	The Reliability Coordinator failed to monitor **all** Bulk Electric System facilities, which may include sub-	The Reliability Coordinator failed to monitor Bulk Electric System facilities, which may include sub-transmission

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.			transmission information, within its Reliability Coordinator Area and adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.	information, within adjacent Reliability Coordinator Areas, as necessary to ensure that, at any time, regardless of prior planned or unplanned events, the Reliability Coordinator is able to determine any potential System Operating Limit and Interconnection Reliability Operating Limit violations within its Reliability Coordinator Area.
IRO-003-2	R2.	Each Reliability Coordinator shall know the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation. Reliability Coordinators shall also know the status of any facilities that may be required to assist area restoration objectives.	N/A	N/A	The Reliability Coordinator failed to know either the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation or the status of any facilities that may be required to assist area restoration objectives.	The Reliability Coordinator failed to know the current status of all critical facilities whose failure, degradation or disconnection could result in an SOL or IROL violation and the status of any facilities that may be required to assist area restoration objectives.
IRO-006-5	R1.	Each Reliability Coordinator and Balancing Authority that receives a request pursuant to an Interconnection-wide transmission loading relief procedure (such as Eastern Interconnection TLR, WECC Unscheduled Flow Mitigation, or congestion management procedures from the ERCOT Protocols) from	N/A	N/A	N/A	The responsible entity received a request to curtail an Interchange Transaction crossing an Interconnection boundary pursuant to an Interconnection-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		any Reliability Coordinator, Balancing Authority, or Transmission Operator in another Interconnection to curtail an Interchange Transaction that crosses an Interconnection boundary shall comply with the request, unless it provides a reliability reason to the requestor why it cannot comply with the request.				wide transmission loading relief procedure from a Reliability Coordinator, Balancing Authority, or Transmission Operator, but the entity neither complied with the request, nor provided a reliability reason why it could not comply with the request.
IRO-006-EAST-1	R1.	When acting or instructing others to act to mitigate the magnitude and duration of the instance of exceeding an IROL within that IROL's TV, each Reliability Coordinator shall initiate, prior to or concurrently with the initiation of the Eastern Interconnection TLR procedure (or continuing management of this procedure if already initiated), one or more of the following actions: • Inter-area redispatch of generation • Intra-area redispatch of generation • Reconfiguration of the transmission system • Voluntary load reductions (e.g., Demand-side Management) • Controlled load reductions (e.g., load shedding)	N/A	N/A	N/A	When acting or instructing others to act to mitigate the magnitude and duration of the instance of exceeding an IROL within that IROL's Tv, the Reliability Coordinator did not initiate one or more of the actions listed under R1 prior to or in conjunction with the initiation of the Eastern Interconnection TLR procedure (or continuing management of this procedure if already initiated).
IRO-006-EAST-1	R2.	To ensure operating entities are provided with information needed to maintain an	The Reliability Coordinator initiating	The Reliability Coordinator	The Reliability Coordinator initiating	The Reliability Coordinator initiating

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		awareness of changes to the Transmission System, when initiating the Eastern Interconnection TLR procedure to prevent or mitigate an SOL or IROL exceedance, and at least every clock hour (with the exception of TLR-1, where an hourly update is not required) after initiation up to and including the hour when the TLR level has been identified as TLR Level 0, the Reliability Coordinator shall identify: 2.1. A list of congestion management actions to be implemented, and 2.2. One of the following TLR levels: TLR-1, TLR-2, TLR-3A, TLR-3B, TLR-4, TLR-5A, TLR-5B, TLR-6, TLR-0	the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for one clock hour during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.	initiating the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for two clock hours during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.	the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for three clock hours during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.	the Eastern Interconnection TLR procedure missed identifying the TLR Level and/or a list of congestion management actions to take as specified by the requirement for four or more clock hours during the period from initiation up to the hour when the TLR level was identified as TLR Level 0.
IRO-006-EAST-1	R3.	Upon the identification of the TLR level and a list of congestion management actions to be implemented, the Reliability Coordinator initiating this TLR procedure shall: o Notify all Reliability Coordinators in the Eastern Interconnection of the identified TLR level o Communicate the list of congestion management actions to be implemented to 1.) all Reliability Coordinators in the Eastern Interconnection, and 2.) those Reliability Coordinators in other Interconnections responsible for curtailing Interchange Transactions crossing Interconnection boundaries identified in the list of congestion management actions. o Request that the congestion management actions identified in Requirement R2, Part 2.1 be	The initiating Reliability Coordinator did not notify one or more Reliability Coordinators in the Eastern Interconnection of the TLR Level (3.1).	N/A	The initiating Reliability Coordinator did not communicate the list of congestion management actions to one or more of the Reliability Coordinators listed in Requirement R3, Part 3.2. OR The initiating Reliability Coordinator requested some, but not all, of the Reliability Coordinators identified in Requirement R3, Part 3.3 to implement the identified	The initiating Reliability Coordinator requested none of the Reliability Coordinators identified in Requirement R3, Part 3.3 to implement the identified congestion management actions.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implemented by: 1.) Each Reliability Coordinator associated with a Sink Balancing Authority for which Interchange Transactions are to be curtailed, 2.) Each Reliability Coordinator associated with a Balancing Authority in the Eastern Interconnection for which Network Integration Transmission Service or Native Load is to be curtailed, and 3.) Each Reliability Coordinator associated with a Balancing Authority in the Eastern Interconnection for which its Market Flow is to be curtailed.			congestion management actions.	
IRO-006-EAST-1	R4.	Each Reliability Coordinator that receives a request as described in Requirement R3, Part 3.3. shall, within 15 minutes of receiving the request, implement the congestion management actions requested by the issuing Reliability Coordinator as follows: • Instruct its Balancing Authorities to implement the Interchange Transaction schedule change requests. • Instruct its Balancing Authorities to implement the Network Integration Transmission Service and Native Load schedule changes for which the Balancing Authorities are responsible. • Instruct its Balancing Authorities to implement the Market Flow schedule changes for which the Balancing Authorities are responsible. • If an assessment determines shows that	N/A	N/A	N/A	The responding Reliability Coordinator did not, within 15 minutes of receiving a request, either 1.) implement all the requested congestion management actions, or 2.) implement none or some of the requested congestion management actions and replace the remainder with alternate congestion management actions, provided that: assessment showed that the actions replaced would have

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		one or more of the congestion management actions communicated in Requirement R3, Part 3.3 will result in a reliability concern or will be ineffective, the Reliability Coordinator may replace those specific actions with alternate congestion management actions, provided that: o The alternate congestion management actions have been agreed to by the initiating Reliability Coordinator, and o The assessment shows that the alternate congestion management actions will not adversely affect reliability.				resulted in a reliability concern or would have been ineffective, the alternate congestion management actions were agreed to by the initiating Reliability Coordinator, and assessment determined that the alternate congestion management actions would not adversely affect reliability.
IRO-006-TRE-1	R1.	The RC shall have procedures to identify and mitigate exceedances of identified Interconnection Reliability Operating Limits (IROL) and System Operating Limits (SOL) that will not be resolved by the automatic actions of the ERCOT Nodal market operations system. The procedures shall address, but not be limited to, one or more of the following: redispatch of generation; reconfiguration of the Transmission system; controlled load reductions (including both firm and non-firm load shedding).	N/A	N/A	N/A	The RC did not have procedures to identify and mitigate exceedances of identified IROLs and SOLs.
IRO-006-TRE-1	R2.	The RC shall act to identify and mitigate exceedances of identified Interconnection Reliability Operating Limits and System Operating Limits that will not be resolved by the automatic actions of the ERCOT Nodal market operations system, in accordance with the procedures required by R1.	N/A	N/A	The RC failed to follow its procedures in identifying and mitigating an exceedance of an SOL.	The RC failed to follow its procedures in identifying and mitigating an exceedance of an IROL.

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-006-WECC-1	R1.	Upon receiving a request of Step 4 or greater (see Attachment 1-IRO-006-WECC-1) from the Transmission Operator of a Qualified Transfer Path, the Reliability Coordinator shall approve (actively or passively) or deny that request within five minutes.	There shall be a Lower Level of non-compliance if there is one instance during a calendar month in which the Reliability Coordinator approved (actively or passively) or denied a Step 4 or greater request greater than five minutes after receipt of notification from the Transmission Operator of a Qualified Transfer Path.	N/A	N/A	N/A
IRO-006-WECC-1	R2.	The Balancing Authorities shall approve curtailment requests to the schedules as submitted, implement alternative actions, or a combination there of that collectively meets the Relief Requirement.	There shall be a Lower Level of non-compliance if there is less than 100% Relief Requirement provided but greater than or equal to 90% Relief Requirement provided or the Relief Requirement was less than 5 MW and was not provided.	There shall be a Moderate Level of non-compliance if there is less than 90% Relief Requirement provided but greater than or equal to 75% Relief Requirement provided and the Relief Requirement was greater than 5 MW and was not provided.	There shall be a High Level of non-compliance if there is less than 75% Relief Requirement provided but greater than or equal to 60% Relief Requirement provided and the Relief Requirement was greater than 5 MW and was not provided.	There shall be a Severe Level of non-compliance if there is less than 60% Relief Requirement provided and the Relief Requirement was greater than 5 MW and was not provided.
IRO-014-1	R1.	The Reliability Coordinator shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability. These Operating Procedures, Processes, or Plans shall address Scenarios	N/A	N/A	The Reliability Coordinator has Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or	The Reliability Coordinator failed to have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that affect other Reliability Coordinator Areas as well as those developed in coordination with other Reliability Coordinators.			coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability, but failed to address Scenarios that affect other Reliability Coordinator Areas.	coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability.
IRO-014-1	R1.1.	These Operating Procedures, Processes, or Plans shall collectively address, as a minimum, the following:	N/A	The Reliability Coordinator failed to include one of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in its Operating Procedures, Processes, or Plans.	The Reliability Coordinator failed to include two of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in its Operating Procedures, Processes, or Plans.	The Reliability Coordinator failed to include more than two of the elements listed in IRO-014-1 R1.1.1 through R1.1.6 in its Operating Procedures, Processes, or Plans.
IRO-014-1	R1.1.1.	Communications and notifications, including the conditions under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.2.	Energy and capacity shortages.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.3.	Planned or unplanned outage information.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.4.	Voltage control, including the coordination of reactive resources for voltage control.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.5.	Coordination of information exchange to support reliability assessments.	N/A	N/A	N/A	N/A
IRO-014-1	R1.1.6.	Authority to act to prevent and mitigate instances of causing Adverse Reliability Impacts to other Reliability Coordinator Areas.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (IRO)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
IRO-014-1	R2.	Each Reliability Coordinator's Operating Procedure, Process, or Plan that requires one or more other Reliability Coordinators to take action (e.g., make notifications, exchange information, or coordinate actions) shall be:	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R2.1 or R2.2.
IRO-014-1	R2.1.	Agreed to by all the Reliability Coordinators required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not agreed to by all the Reliability Coordinators required to take the indicated action(s).
IRO-014-1	R2.2.	Distributed to all Reliability Coordinators that are required to take the indicated action(s).	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan was not distributed to all Reliability Coordinators that are required to take the indicated action(s).
IRO-014-1	R3.	A Reliability Coordinator's Operating Procedures, Processes, or Plans developed to support a Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan shall include:	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to comply with either IRO-014-1 R3.1 or R3.2.
IRO-014-1	R3.1.	A reference to the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to reference the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R3.2.	The agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.	N/A	N/A	N/A	The Reliability Coordinator's Operating Procedure, Process, or Plan failed to include the agreed-upon actions from the associated Reliability Coordinator-to-Reliability Coordinator Operating Procedure, Process, or Plan.
IRO-014-1	R4.	Each of the Operating Procedures, Processes, and Plans addressed in Reliability Standard IRO-014 Requirement 1 and Requirement 3 shall:	N/A	The Operating Procedures, Processes and Plans did not include **one** of the elements listed in IRO-014-1 R4.1 through R4.3.	The Operating Procedures, Processes and Plans did not include **two** of the elements listed in IRO-014-1 R4.1 through R4.3.	The Operating Procedures, Processes and Plans did not include **any** of the elements listed in IRO-014-1 R4.1 through R4.3.
IRO-014-1	R4.1.	Include version control number or date	N/A	N/A	N/A	N/A
IRO-014-1	R4.2.	Include a distribution list.	N/A	N/A	N/A	N/A
IRO-014-1	R4.3.	Be reviewed, at least once every three years, and updated if needed.	N/A	N/A	N/A	N/A
IRO-015-1	R1.	The Reliability Coordinator shall follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making	N/A	The Reliability Coordinator failed to follow its Operating Procedures, Processes, or Plans for making notifications and exchanging reliability-

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notifications and exchanging reliability-related information with other Reliability Coordinators but no adverse reliability impacts resulted from the incident.		related information with other Reliability Coordinators and adverse reliability impacts resulted from the incident.
IRO-015-1	R1.1.	The Reliability Coordinator shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas.	N/A	The Reliability Coordinator failed to make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas but no adverse reliability impacts resulted from the incident.	N/A	The Reliability Coordinator failed to make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas and adverse reliability impacts resulted from the incident.
IRO-015-1	R2.	The Reliability Coordinator shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.	N/A	N/A	N/A	The Reliability Coordinator failed to participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.
IRO-015-1	R2.1.	The frequency of these conference calls shall be agreed upon by all involved Reliability Coordinators and shall be at least weekly.	N/A	N/A	N/A	The Reliability Operator failed to participate in the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment of the need and frequency of conference calls with other Reliability Operators.
IRO-015-1	R3.	The Reliability Coordinator shall provide reliability-related information as requested by other Reliability Coordinators.				The Reliability Coordinator failed to provide reliability-related information as requested by other Reliability Coordinators.
IRO-016-1	R1.	The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.	The Reliability Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators, contacted the other Reliability Coordinator(s) to confirm that there was a problem, discussed options and decided upon a solution to prevent or resolve the identified problem, but failed to have evidence that it coordinated with other Reliability Coordinators.	N/A	N/A	The Reliability Coordinator that identified a potential, expected, or actual problem that required the actions of one or more other Reliability Coordinators failed to contact the other Reliability Coordinator(s) to confirm that there was a problem, discuss options and decide upon a solution to prevent or resolve the identified problem.
IRO-016-1	R1.1.	If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall	The responsible entity agreed on the problem and the actions to take to prevent or mitigate	N/A	N/A	The responsible entity agreed on the problem and the actions to take to prevent or mitigate

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.	the system condition, implemented the agreed-upon solution, but failed to notify the involved Reliability Coordinators of the action(s) taken.			the system condition, but failed to implement the agreed-upon solution.
IRO-016-1	R1.2.	If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).	N/A	N/A	N/A	The involved Reliability Coordinators could not agree on the problem(s), but a Reliability Coordinator failed to re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).
IRO-016-1	R1.2.1.	If time permits, this re-evaluation shall be done before taking corrective actions.	N/A	N/A	N/A	The Reliability Coordinator failed to re-evaluate the problem prior to taking corrective actions, during periods when time was not an issue.
IRO-016-1	R1.2.2.	If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.	N/A	N/A	N/A	The Reliability Coordinator failed to operate as though the problem(s) exist(s) until the conflicting system status was resolved, during periods when time was an issue.
IRO-016-1	R1.3.	If the involved Reliability Coordinators cannot agree on the solution, the more	N/A	N/A	N/A	The Reliability Coordinator

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		conservative solution shall be implemented.				implemented a solution other than the most conservative solution, when agreement on the solution could not be reached.
IRO-016-1	R2. (Retired)	The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.	N/A	N/A	N/A	The Reliability Coordinator failed to document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-010-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R 1	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to 50% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics, system data, and existing and future Interchange Schedules in compliance with its respective Interconnection Regional steady-state modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-011-0_R1.
MOD-010-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-011-0_R1) shall provide this steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. If no schedule exists, then	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the steady-state modeling and simulation data to	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than or equal to	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than or equal to 75% of the steady-state modeling	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the steady-state modeling and simulation data to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		these entities shall provide the data on request (30 calendar days).	the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 30 but less than or equal to 35 calendar days following the request.	50% of the steady-state modeling and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.	and simulation data to the Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 40 but less than or equal to 45 calendar days following the request.	Regional Reliability Organizations, NERC, and those entities specified within Reliability Standard MOD-011-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide data more than 45 calendar days following the request.
MOD-012-0	R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R1) shall provide appropriate equipment characteristics and system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the appropriate equipment characteristics and system data in compliance with the respective	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the appropriate equipment characteristics and	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the appropriate equipment characteristics and system data in compliance with the	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the appropriate equipment characteristics and system data in compliance with the respective

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1	system data in compliance with the respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	respective Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.	Interconnection-wide Regional dynamics system modeling and simulation data requirements and reporting procedures as defined in Reliability Standard MOD-013-0_R1.
MOD-012-0	R2.	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners (specified in the data requirements and reporting procedures of MOD-013-0_R4) shall provide dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. If no schedule exists, then these entities shall provide data on request (30 calendar days).	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide less than or equal to 25% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1 OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 25% but less than 50% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule exists, The	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 50% but less than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data	The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to provide greater than 75% of the dynamics system modeling and simulation data to its Regional Reliability Organization(s), NERC, and those entities specified within the applicable reporting procedures identified in Reliability Standard MOD-013-0_R 1. OR If no schedule exists, The Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Planners provided data more than 30 but less than or equal to 35 calendar days following the request.	Transmission Owners, Transmission Planners, Generator Owners, and Resource Planners provided data more than 35 but less than or equal to 40 calendar days following the request.	more than 40 but less than or equal to 45 calendar days following the request.	provide data more than 45 calendar days following the request.
MOD-016-1.1	R1.	The Planning Authority and Regional Reliability Organization shall have documentation identifying the scope and details of the actual and forecast (a) Demand data, (b) Net Energy for Load data, and (c) controllable DSM data to be reported for system modeling and reliability analyses.	N/A	The responsible entity did not have documentation identifying the scope and details of the actual and forecast data for one (1) of the following types of data to be reported for system modeling and reliability analyses: • Demand data • Net Energy for Load data • Controllable DSM data	The responsible entity did not have documentation identifying the scope and details of the actual and forecast data for two (2) of the following to be reported for system modeling and reliability analyses: • Demand data • Net Energy for Load data • Controllable DSM data	The responsible entity did not have documentation identifying the scope and details of the actual and forecast data to be reported for system modeling and reliability analyses.
MOD-016-1.1	R1.1.	The aggregated and dispersed data submittal requirements shall ensure that consistent data is supplied for Reliability Standards TPL-005, TPL-006, MOD-010, MOD-011, MOD-012, MOD-013, MOD-014, MOD-015, MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, and MOD-021. The data submittal requirements shall stipulate that	The responsible entity failed to ensure that consistent data is supplied for one of the Reliability Standards as specified in R1.1.	The responsible entity failed to ensure that consistent data is supplied for two of the Reliability Standards as specified in R1.1.	The responsible entity failed to ensure that consistent data is supplied for three of the Reliability Standards as specified in R1.1.	The responsible entity failed to ensure that consistent data is supplied for four or more of the Reliability Standards as specified in R1.1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.				OR The responsible entity failed to stipulate that each Load-Serving Entity count its customer Demand once and only once, on an aggregated and dispersed basis, in developing its actual and forecast customer Demand values.
MOD-016-1.1	R2.	The Regional Reliability Organization shall distribute its documentation required in Requirement 1 and any changes to that documentation, to all Planning Authorities that work within its Region.	N/A	N/A	The Regional Reliability Organization distributed its documentation as specified in R1 but failed to distribute any changes to that documentation, to all Planning Authorities that work within its Region.	The Regional Reliability Organization failed to distribute its documentation as specified in R1 to all Planning Authorities that work within its Region.
MOD-016-1.1	R2.1.	The Regional Reliability Organization shall make this distribution within 30 calendar days of approval.	The Regional Reliability Organization distributed the documentation more than 30 but less than or equal to 37 calendar days following approval.	The Regional Reliability Organization made the distribution more than 37 but less than or equal to 51 calendar days following approval.	The Regional Reliability Organization made the distribution more than 51 but less than or equal to 58 calendar days following approval.	The Regional Reliability Organization failed to make the distribution more than 58 calendar days following approval.
MOD-016-1.1	R3.	The Planning Authority shall distribute its documentation required in R1 for reporting customer data and any changes to that documentation, to its Transmission Planners and	The responsible entity failed to distribute its documentation required in Requirement R1 and	The responsible entity failed to distribute its documentation required in	The responsible entity failed to distribute its documentation required in Requirement R1 and any changes to that	The responsible entity failed to distribute its documentation as specified in Requirement R1 to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Load-Serving Entities that work within its Planning Authority Area.	any changes to that documentation to 5% or less of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity distributed the documentation more than 30 calendar days but less than or equal to 40 calendar days following approval.	Requirement R1 and any changes to that documentation to more than 5% up to (and including) 10% of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity made the distribution more than 40 calendar days but less than or equal to 50 calendar days following approval.	documentation to more than 10% up to (and including) 15% of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity made the distribution more than 50 calendar days but less than or equal to 60 calendar days following approval.	more than 15% of all Transmission Planners and Load-Serving Entities that work within its Region. OR The responsible entity failed to make the distribution more than 60 calendar days following approval.
MOD-016-1.1	R3.1.	The Planning Authority shall make this distribution within 30 calendar days of approval.	N/A	N/A	N/A	N/A
MOD-017-0.1	R1.	The Load-Serving Entity, Planning Authority, and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R 1.	The responsible entity failed to provide one (1) of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The responsible entity failed to provide two (2) of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The responsible entity failed to provide three (3) of the elements of information as specified in R1.1, R1.2, R1.3 or R1.4 on an annual basis.	The responsible entity failed to provide all of the elements of information as specified in R1.1, R1.2, R1.3 and R1.4 on an annual basis.
MOD-017-0.1	R1.1.	Integrated hourly demands in megawatts (MW) for the prior year.	N/A	N/A	N/A	N/A
MOD-017-0.1	R1.2.	Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
MOD-017-0.1	R1.3.	Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.	N/A	N/A	N/A	N/A
MOD-017-0.1	R1.4.	Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.	N/A	N/A	N/A	N/A
MOD-018-0	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or dispersed basis) shall:	N/A	The responsible entity's report failed to include one (1) of the items as specified in R1.1, R1.2, or R1.3.	The responsible entity's report failed to include two (2) of the items as specified in R1.1, R1.2, or R1.3.	The responsible entity's report failed to include any of the items as specified in R1.1, R1.2, and R1.3.
MOD-018-0	R1.1.	Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and	N/A	N/A	N/A	N/A
MOD-018-0	R1.2.	Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load.	N/A	N/A	N/A	N/A
MOD-018-0	R1.3.	Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1.	N/A	N/A	N/A	N/A
MOD-018-0	R2.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days).	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner reported the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to report the data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 30 but less than or equal to 45 calendar days following the request.	NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 45 but less than or equal to 60 calendar days following the request.	Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 60 but less than or equal to 75 calendar days following the request.	Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner more than 75 calendar days following the request.
MOD-019-0.1	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R 1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually less than or equal to 25% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 25% but less than or equal to 50% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 50% but less than or equal to 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to provide annually greater than 75% of the interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			MOD-016-0_R 1.	Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-0_R1.	MOD-016-0_R1.	MOD-016-0_R1.
MOD-020-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 30 but less than 45 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 45 but less than 60 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner made known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 60 but less than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner failed to make known its amount of interruptible demands and Direct Control Load Management (DCLM) more than 75 calendar days following the request from Transmission Operators, Balancing Authorities, and Reliability Coordinators.
MOD-021-1	R1.	The Load-Serving Entity, Transmission Planner and Resource Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed.	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how one (1)	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts document how the Demand and energy effects of DSM programs but failed to document how three (3) of the following	Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts failed to document how the Demand and energy effects of DSM programs are addressed.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	document how two (2) of the following elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	elements of the Demand and energy effects of DSM programs are addressed: conservation, time-of-use rates, interruptible Demands or Direct Control Load Management.	
MOD-021-1	R2.	The Load-Serving Entity, Transmission Planner and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R1.	N/A	N/A	N/A	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R 1.
MOD-021-1	R3.	The Load-Serving Entity, Transmission Planner and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days).	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 30 but less than 45 calendar days	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 45 but	The Load-Serving Entity, Transmission Planner, and Resource Planner provided documentation on the treatment of its DSM programs more than 60 but less than 75 calendar days following	The Load-Serving Entity, Transmission Planner, and Resource Planner failed to provide documentation on the treatment of its DSM programs more than 75 calendar days following the request

Complete Violation Severity Level Matrix (MOD)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			following the request from NERC.	less than 60 calendar days following the request from NERC.	the request from NERC.	from NERC.

Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-2	R1.	The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt.	The Nuclear Plant Generator Operator provided the NPIR's to the applicable entities but did not verify receipt.	The Nuclear Plant Generator Operator did not provide the proposed NPIR to one of the applicable entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to two of the applicable entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to more than two of applicable entities.
NUC-001-2	R2.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.	N/A	N/A	N/A	The Nuclear Plant Generator Operator or the applicable Transmission Entity does not have in effect one or more agreements that include mutually agreed to NPIRs and document the implementation of the NPIRs.
NUC-001-2	R3.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator.	N/A	The responsible entity incorporated the NPIRs into its planning analyses but did not communicate the results to the Nuclear Plant Generator Operator.	N/A	The responsible entity did not incorporate the NPIRs into its planning analyses of the electric system.
NUC-001-2	R4.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall:	The applicable Transmission Entity failed to incorporate one or more applicable NPIRs into their operating analyses.	The applicable Transmission Entity failed to incorporate any NPIRs into their operating analyses OR did not inform NPG operator when their ability of	The applicable Transmission Entity failed to operate the system to meet the NPIRs	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assess the operation of the electric system affecting the NPIRs was lost.		
NUC-001-2	R4.1	Incorporate the NPIRs into their operating analyses of the electric system.	N/A	N/A	N/A	N/A
NUC-001-2	R4.2	Operate the electric system to meet the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R4.3	Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.	N/A	N/A	N/A	N/A
NUC-001-2	R5.	The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard.	N/A	N/A	N/A	The Nuclear Plant Generator Operator failed to operate per the Agreements developed in accordance with this standard.
NUC-001-2	R6.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs.	The Nuclear Operator or Transmission Entity failed to coordinate outages or maintenance activities in accordance with one or more of the administrative elements within the agreements.	The Nuclear Operator or Transmission Entity failed to provide outage or maintenance schedules to the appropriate parties as described in the agreement or on a time period consistent with the agreements.	The Nuclear Operator or Transmission Entity failed to coordinate one or more outages or maintenance activities in accordance the requirements of the agreements.	N/A
NUC-001-2	R7.	Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design,	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities	The Nuclear Plant Generator Operator did not inform the applicable Transmission	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	of proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	Entities of actual changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	of actual changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that directly impact the ability of the electric system to meet the NPIRs.	
NUC-001-2	R8.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of proposed changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that directly impacts the ability of the electric system to meet the NPIRs.	N/A
NUC-001-2	R9.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2:	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing one or more sub-components of R9.1.	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from one to five of the combined sub-	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing from six to ten of the combined sub-components in R9.2,	The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing eleven or more of the combined sub-components in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Retired)	components in R9.2, R9.3 and R9.4.	R9.3 and R9.4.	R9.2, R9.3 and R9.4.
NUC-001-2	R9.1 (Retired)	Administrative elements:	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.1 (Retired)	Definitions of key terms used in the agreement.	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.2 (Retired)	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.3 (Retired)	A requirement to review the agreement(s) at least every three years.	N/A	N/A	N/A	N/A
NUC-001-2	R9.1.4 (Retired)	A dispute resolution mechanism.	N/A	N/A	N/A	N/A
NUC-001-2	R9.2	Technical requirements and analysis:	N/A	N/A	N/A	N/A
NUC-001-2	R9.2.1	Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.	N/A	N/A	N/A	N/A
NUC-001-2	R9.2.2	Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.2.3	Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3	Operations and maintenance coordination:	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.1	Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		responsibilities for operational control coordination and maintenance of these facilities.				
NUC-001-2	R9.3.2	Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.3	Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.4	Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.5	Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.6	Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.	N/A	N/A	N/A	N/A
NUC-001-2	R9.3.7	Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4	Communications and training:	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (NUC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
NUC-001-2	R9.4.1	Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.2	Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.3	Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.4	Provisions for supplying information necessary to report to government agencies, as related to NPIRs.	N/A	N/A	N/A	N/A
NUC-001-2	R9.4.5	Provisions for personnel training, as related to NPIRs.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-001-0.2	R1.	Each Transmission Operator and Balancing Authority shall provide operating personnel with the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	N/A	N/A	The Transmission Operator or Balancing Authority failed to demonstrate that it communicated to its operating personnel their responsibility or their authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	The Transmission Operator or Balancing Authority failed to demonstrate that it communicated to its operating personnel their responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.
PER-002-0	R1.	Each Transmission Operator and Balancing Authority shall be staffed with adequately trained operating personnel.	The responsible entity failed to staff 5% or less with adequately trained operating personnel.	The responsible failed to staff more than 5% up to (and including) 10% with adequately trained operating personnel.	The responsible entity failed to staff more than 10% up to (and including) 15% with adequately trained operating personnel.	The responsible entity failed to staff more than 15% with adequately trained operating personnel.
PER-002-0	R2.	Each Transmission Operator and Balancing Authority shall have a training program for all operating personnel that are in:	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting 5% or less of its operating personnel.	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting more than 5% up to (and including) 10% of its operating personnel.	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting more than 10% up to (and including) 15% of its operating personnel.	The responsible entity did not train operating personnel for positions described in R2.1 or R2.2, affecting more than 15% of its operating personnel.
PER-002-0	R2.1.	Positions that have the primary responsibility, either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System.	N/A	N/A	N/A	N/A
PER-002-0	R2.2.	Positions directly responsible for complying with NERC standards.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-002-0	R3.	For personnel identified in Requirement R2, the Transmission Operator and Balancing Authority shall provide a training program meeting the following criteria:	The applicable entity did not comply with one of the four required elements.	The applicable entity did not comply with two of the four required elements.	The applicable entity did not comply with three of the four required elements.	The applicable entity did not comply with any of the four required elements.
PER-002-0	R3.1.	A set of training program objectives must be defined, based on NERC and Regional Reliability Organization standards, entity operating procedures, and applicable regulatory requirements. These objectives shall reference the knowledge and competencies needed to apply those standards, procedures, and requirements to normal, emergency, and restoration conditions for the Transmission Operator and Balancing Authority operating positions.	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for less than 25% of the applicable BA and TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 25% or more but less than 50% of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 50% or more but less than 75% of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)	The responsible entity's training program objectives were incomplete (e.g. The responsible entity failed to define training program objectives for 75% or more of the applicable BA & TOP NERC and Regional Reliability Organizations standards, entity operating procedures, and regulatory requirements.)
PER-002-0	R3.2.	The training program must include a plan for the initial and continuing training of Transmission Operator and Balancing Authority operating personnel. That plan shall address knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the	The responsible entity does not have a plan for continuing training of operating personnel. OR The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. OR The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.	The responsible entity does not have a plan for continuing training of operating personnel. AND The responsible entity does not have a plan for initial training of operating personnel. AND The responsible entity's plan does not address the knowledge and competencies required for reliable system operations.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			knowledge and competencies required for reliable system operations.	knowledge and competencies required for reliable system operations.		
PER-002-0	R3.3.	The training program must include training time for all Transmission Operator and Balancing Authority operating personnel to ensure their operating proficiency.	The responsible entity has produced the training program with more than 75% but less than 100% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 50% but less than or equal to 75% of operating personnel provided with training time.	The responsible entity has produced the training program with more than 25% but less than or equal to 50% of operating personnel provided with training time.	The responsible entity has produced the training program with more than or equal to 0% but less than or equal to 25% of operating personnel provided with training time.
PER-002-0	R3.4.	Training staff must be identified, and the staff must be competent in both knowledge of system operations and instructional capabilities.	N/A	The responsible entity has produced the training program with training staff identified that lacks knowledge of system operations. OR The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	The responsible entity has produced the training program with training staff identified that lacks knowledge of system operations. AND The responsible entity has produced the training program with training staff identified that lacks instructional capabilities.	The responsible entity has produced the training program with no training staff identified.
PER-003-1	R1.	Each Reliability Coordinator shall staff its Real-time operating positions performing Reliability Coordinator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining a valid NERC Reliability Operator				The Reliability Coordinator failed to staff each Real-time operating position performing Reliability Coordinator reliability-related

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		certificate:				tasks with a System Operator having a valid NERC certificate as defined in Requirement R1.
PER-003-1	R2.	Each Transmission Operator shall staff its Real-time operating positions performing Transmission Operator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates:				The Transmission Operator failed to staff each Real-time operating position performing Transmission Operator reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R2, Part 2.2.
PER-003-1	R3.	Each Balancing Authority shall staff its Real-time operating positions performing Balancing Authority reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates:				The Balancing Authority failed to staff each Real-time operating position performing Balancing Authority reliability-related tasks with a System Operator having a valid NERC certificate as defined in Requirement R3, Part 3.2.

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PER-004-1	R3.	Reliability Coordinator operating personnel shall have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	5% or less of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	More than 5% up to (and including) 10% of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	More than 10% up to (and including) 15% of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.	More than 15% of the Reliability Coordinator operating personnel did not have a comprehensive understanding of the Reliability Coordinator Area and interactions with neighboring Reliability Coordinator Areas.
PER-004-1	R4.	Reliability Coordinator operating personnel shall have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.	5% or less of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and	More than 5% up to (and including) 10% of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment	More than 10% up to (and including) 15% of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.	More than 15% of the Reliability Coordinator operating personnel did not have an extensive understanding of the Balancing Authorities, Transmission Operators, and Generation Operators within the Reliability Coordinator Area, including the operating staff, operating practices and procedures, restoration priorities and objectives, outage plans, equipment capabilities, and operational restrictions.

Complete Violation Severity Level Matrix (PER)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			operational restrictions.	capabilities, and operational restrictions.		

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-001-1	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.	N/A	N/A	The responsible entity failed to be familiar with the limitations of protection system schemes applied in its area.	The responsible entity failed to be familiar with the purpose of protection system schemes applied in its area.
PRC-001-1	R2.	Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:	N/A	N/A	N/A	The responsible entity failed to notify any reliability entity of relay or equipment failures.
PRC-001-1	R2.1.	If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, but corrective action was taken.	Notification of relay or equipment failure was made to the Transmission Operator and Host Balancing Authority, but corrective action was not taken.	Notification of relay or equipment failure was not made to the Transmission Operator and Host Balancing Authority, and corrective action was not taken.
PRC-001-1	R2.2.	If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.	N/A	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing Authorities, but corrective action was taken.	Notification of relay or equipment failure was made to the Reliability Coordinator and affected Transmission Operators and Balancing Authorities, but corrective action was not taken.	Notification of relay or equipment failure was not made to the Reliability Coordinator and affected Transmission Operators and Balancing Authorities, and corrective action was not taken.
PRC-001-1	R3.	A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-001-1	R3.1.	Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.	The Generator Operator failed to coordinate one new protective system or protective system change with either its Transmission Operator or its Host Balancing Authority or both.	The Generator Operator failed to coordinate two new protective systems or protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate three new protective systems or protective system changes with either its Transmission Operator or its Host Balancing Authority, or both.	The Generator Operator failed to coordinate more than three new protective systems or protective system changes with its Transmission Operator or its Host Balancing Authority, or both.
PRC-001-1	R3.2.	Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.	The Transmission Operator failed to coordinate one new protective system or protective system change with neighboring Transmission Operators or Balancing Authorities or both.	The Transmission Operator failed to coordinate two new protective systems or protective system changes with neighboring Transmission Operators or Balancing Authorities or both.	The Transmission Operator failed to coordinate three new protective systems or protective system changes with neighboring Transmission Operators or Balancing Authorities or both.	The Transmission Operator failed to coordinate more than three new protective systems or protective system changes with neighboring Transmission Operators or Balancing Authorities or both.
PRC-001-1	R4.	Each Transmission Operator shall coordinate protection systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with one of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with two of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with three of its neighboring Generator Operators, Transmission Operators, or Balancing Authorities.	The Transmission Operator failed to coordinate protection systems on major transmission lines and interconnections with three or more of its neighboring Generator Operators, Transmission Operators, and Balancing Authorities.
PRC-001-1	R5.	A Generator Operator or Transmission Operator shall coordinate changes in	N/A	N/A	The Generator Operator failed to notify its	The Generator Operator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		generation, transmission, load or operating conditions that could require changes in the protection systems of others:			Transmission Operator at all of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems. (R5.1) OR The Transmission Operator failed to notify neighboring Transmission Operators at all of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems. (R5.2)	notify its Transmission Operator at all of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems. (R5.1) AND The Transmission Operator failed to notify neighboring Transmission Operators at all of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems. (R5.2)
PRC-001-1	R5.1.	Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.	N/A	N/A	N/A	N/A
PRC-001-1	R5.2.	Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.	N/A	N/A	N/A	N/A
PRC-001-1	R6.	Each Transmission Operator and Balancing Authority shall monitor the status of each	N/A	N/A	The responsible entity monitored the status of	The responsible entity failed to monitor the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.			each Special Protection System in its area but notification of a change in status of a Special Protection System was not made to the affected Transmission Operators and Balancing Authorities.	status of each Special Protection System in its area, and did not notify affected Transmission Operators and Balancing Authorities of each change in status.
PRC-002-NPCC-01	R1.	Each Transmission Owner and Generator Owner shall provide Sequence of Event (SOE) recording capability by installing Sequence of Event recorders or as part of another device, such as a Supervisory Control And Data Acquisition (SCADA) Remote Terminal Unit (RTU), a generator plant Digital (or Distributed) Control System (DCS) or part of Fault recording equipment. This capability shall: [See standard for requirements of SOE recording capability]	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed up to and including 10% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed more than 10% and up to and including 20% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed more than 20% and up to and including 30% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.	The Transmission Owner or Generator Owner provided the Sequence of Event recording capability meeting the bulk of R1 but missed more than 30% of the total set, which is the product of the total number of locations in 1.1 times the total number of parameters in 1.2.
PRC-002-NPCC-01	R2.	Each Transmission Owner shall provide Fault recording capability for the following Elements at facilities where Fault recording equipment is required to be installed as per R3: [See standard for list of elements]	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed up to and including 10% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the criteria listed in 2.1 through 2.6.	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed more than 10% and up to and including 20% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed more than 20% and up to and including 30% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the criteria listed in 2.1 through 2.6.	The Transmission Owner provided the Fault recording capability meeting the bulk of R2 but missed more than 30% of the total set, which is the total number of Elements at all locations required to be installed as per R3 that meet the criteria listed in 2.1 through 2.6.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				criteria listed in 2.1 through 2.6.		
PRC-002-NPCC-01	R3.	Each Transmission Owner shall have Fault recording capability that determines the Current Zero Time for loss of Bulk Electric System (BES) transmission Elements.	N/A	N/A	N/A	The Transmission Owner failed to provide fault recording capability that determines the current zero time for loss of transmission Elements.
PRC-002-NPCC-01	R4.	Each Generator Owner shall provide Fault recording capability for Generating Plants at and above 200 MVA Capacity and connected through a generator step up (GSU) transformer to a Bulk Electric System Element unless Fault recording capability is already provided by the Transmission Owner.	The Generator Owner failed to provide Fault recording capability at up to and including 10% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.	The Generator Owner failed to provide Fault recording capability at more than 10% and up to and including 20% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.	The Generator Owner failed to provide Fault recording capability at more than 20% and up to 30% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.	The Generator Owner failed to provide Fault recording capability at more than 30% of its Generating Plants at and above 200 MVA Capacity and connected to a Bulk Electric System Element if Fault recording capability for that portion of the system is inadequate.
PRC-002-NPCC-01	R5.	Each Transmission Owner and Generator Owner shall record for Faults, sufficient electrical quantities for each monitored Element to determine the following: [See standard for list]	The Transmission Owner or Generator Owner failed to record for the Faults up to and including 10% of the total set of parameters, which is the product of the total number of monitored Elements and the number of parameters	The Transmission Owner or Generator Owner failed to record for the Faults more than 10% and up to and including 20% of the total set of parameters, which is the product of the total number of monitored Elements	The Transmission Owner or Generator Owner failed to record for the Faults more than 20% and up to and including 30% of the total set of parameters, which is the product of the total number of monitored Elements and the number of parameters	The Transmission Owner or Generator Owner failed to record for the Faults more than 30% of the total set of parameters, which is the product of the total number of monitored Elements and the number of parameters listed in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			listed in 5.1 through 5.5.	and the number of parameters listed in 5.1 through 5.5.	listed in 5.1 through 5.5.	5.1 through 5.5.
PRC-002-NPCC-01	R6.	Each Transmission Owner and Generator Owner shall provide Fault recording with the following capabilities: [See standard for list of capabilities]	The Transmission Owner or Generator Owner failed to provide Fault recording capability for up to and including 10% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of capabilities identified in 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for up to 2 locations.	The Transmission Owner or Generator Owner failed to provide Fault recording capability for more than 10% and up to and including 20% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of capabilities identified in 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for more than two (2) and up to and including five (5) locations.	The Transmission Owner or Generator Owner failed to provide Fault recording capability for more than 20% and up to and including 30% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for more than five (5) and up to and including ten (10) locations.	The Transmission Owner or Generator Owner failed to provide Fault recording capability for more than 30% of the total set of requirements, which is the product of the total number of monitored Elements and the total number of capabilities identified in 6.1 through 6.2. OR Failed to document additional triggers or deviations from the settings stipulated in 6.3 through 6.4 for more than ten (10) locations.
PRC-002-NPCC-01	R7.	Each Reliability Coordinator shall establish its area's requirements for Dynamic Disturbance Recording (DDR) capability that: [See standard for futher requirements]	The Reliability Coordinator failed to establish its area's requirements for up to and including 10% of the required DDR	The Reliability Coordinator failed to establish its area's requirements for more than 10% and up to and including	The Reliability Coordinator failed to establish its area's requirements for more than 20% and up to and including 30% of the	The Reliability Coordinator failed to establish its area's requirements for more than 30% of the required DDR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			coverage for its area as per 7.1and 7.2.	20% of the required DDR coverage for its area as per 7.1 and 7.2.	required DDR coverage for its area as per 7.1 and 7.2.	coverage for its area as per 7.1 and 7.2.
PRC-002-NPCC-01	R8.	Each Reliability Coordinator shall specify that DDRs installed, after the approval of this standard, function as continuous recorders.	N/A	N/A	N/A	The Reliability Coordinator failed to specify that DDRs installed function as continuous recorders.
PRC-002-NPCC-01	R9.	Each Reliability Coordinator shall specify that DDRs are installed with the following capabilities: [See standard for list of capabilities]	N/A	N/A	N/A	The Reliability Coordinator failed to specify that DDRs are installed without the capabilities listed in 9.1 through 9.3.
PRC-002-NPCC-01	R10.	Each Reliability Coordinator shall establish requirements such that the following quantities are monitored or derived where DDRs are installed: [See standard for quantities]	N/A	N/A	N/A	The Reliability Coordinator failed to ensure that the quantities listed in 10.1 through 10.5 are monitored or derived where DDRs are installed.
PRC-002-NPCC-01	R11.	Each Reliability Coordinator shall document additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10, and report this to the Regional Entity (RE) upon request.	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for up to two (2) facilities within the Reliability Coordinator's area	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for more than two (2) and up to five (5)	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for more than five (5) and up to ten (10) facilities within the Reliability Coordinator's area that have a DDR.	The Reliability Coordinator failed to document and report to the Regional Entity upon request additional settings and deviations from the required trigger settings described in R9 and the required list of monitored quantities as described in R10 for more than ten (10) facilities within the Reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			that have a DDR.	facilities within the Reliability Coordinator's area that have a DDR.		Coordinator's area that have a DDR.
PRC-002-NPCC-01	R12.	Each Reliability Coordinator shall specify its DDR requirements including the DDR setting triggers established in R9 to the Transmission Owners and Generator Owners.	N/A	N/A	N/A	The Reliability Coordinator failed to specify to the Transmission Owners and Generator Owners its DDR requirements including the DDR setting triggers established in R9 but missed established setting triggers.
PRC-002-NPCC-01	R13.	Each Transmission Owner and Generator Owner that receives a request from the Reliability Coordinator to install a DDR shall acquire and install the DDR in accordance with R12. Reliability Coordinators, Transmission Owners, and Generator Owners shall mutually agree on an implementation schedule.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for up to and including 10% of the requirement set of the Reliability Coordinator's request to install DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for more than 10% and up to 20% of the requirement set requested by the Reliability Coordinator for installing DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for more than 20% and up to 30% of the requirement set requested by the Reliability Coordinator for installing DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR.	The Transmission Owner or Generator Owner failed to comply with the Reliability Coordinator's request installing the DDR in accordance with R12 for more than 30% of the requirement set requested by the Reliability Coordinator and installing DDRs, with the requirement set being the total number of DDRs requested times the number of setting triggers specified for each DDR OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Reliability Coordinator, Transmission Owners, and Generator Owners failed to mutually agree on an implementation schedule.
PRC-002-NPCC-01	R14.	Each Transmission Owner and Generator Owner shall establish a maintenance and testing program for stand alone DME (equipment whose only purpose is disturbance monitoring) that includes: [See standard for list of inclusions]	The Transmission Owner or Generator Owner established a maintenance and testing program for stand alone DME but provided incomplete data for any one (1) of 14.1 through 14.7.	The Transmission Owner or Generator Owner established a maintenance and testing program for stand alone DME but provided incomplete data for more than one (1) and up to and including three (3) of 14.1 through 14.7.	The Transmission Owner or Generator Owner established a maintenance and testing program for stand alone DME but provided incomplete data for more than three (3) and up to and including six (6) of 14.1 through 14.7.	The Transmission Owner or Generator Owner did not establish any maintenance and testing program for DME; OR The Transmission Owner or Generator Owner established a maintenance and testing program for DME but did not provide any data that meets all of 14.1 through 14.7.
PRC-002-NPCC-01	R15.	Each Reliability Coordinator, Transmission Owner and Generator Owner shall share data within 30 days upon request. Each Reliability Coordinator, Transmission Owner, and Generator Owner shall provide recorded disturbance data from DMEs within 30 days of receipt of the request in each of the following cases: [See standard for the two cases]	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for up to and including fifteen (15) days in	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for more than fifteen (15) days but	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for more than 30 days but less than and including	The Reliability Coordinator, Transmission Owner or Generator Owner provided recorded disturbance data from DMEs but was late for more than forty-five (45) days in meeting

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			meeting the requests of an entity, or entities in 15.1, or 15.2.	less than and including thirty (30) days in meeting the requests of an entity, or entities in 15.1 or 15.2.	forty-five (45) days in meeting the requests of an entity, or entities in 15.1 or 15.2.	the requests of an entity, or entities in 15.1 or 15.2.
PRC-002-NPCC-01	R16.	Each Reliability Coordinator, Transmission Owner and Generator Owner shall submit the data files conforming to the following format requirements: [See standard for format requirements]	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit up to and including two (2) data files in a format that meets the applicable format requirements in 16.1 through 16.3.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit more than two (2) and up to and including five (5) data files in a format that meets the applicable format requirements in 16.1 through 16.3.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit more than five (5) and up to and including ten (10) data files in a format that meets the applicable format requirements in 16.1 through 16.3.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to submit more than ten (10) data files in a format that meets the applicable format requirements in 16.1 through 16.3.
PRC-002-NPCC-01	R17.	Each Reliability Coordinator, Transmission Owner and Generator Owner shall maintain, record and provide to the Regional Entity (RE), upon request, the following data on the DMEs installed to meet this standard: [See standard for types of data]	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request up to and including two (2) of the items in 17.1 through 17.8.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request more than two (2) and up to and including four (4) of the items in 17.1 to 17.8.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request more than four (4) and up to and including six (6) of the items in 17.1 through 17.8.	The Reliability Coordinator, Transmission Owner or Generator Owner failed to maintain or provide to the Regional Entity, upon request more than six (6) of the items in 17.1 through 17.8.
PRC-004-1a	R1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid	N/A	The responsible entity provided evidence of analyzing a Misoperation but the documentation and	N/A	The responsible entity did not perform an analysis of a Misoperation.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for Reliability Standard PRC-003 Requirement 1.		implementation of the associated Corrective Action Plan was not provided.		
PRC-004-1a	R2.	The Generator Owner shall analyze its generator Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	N/A	The Generator Owner provided evidence of analyzing a Misoperation but the documentation and implementation of the associated Corrective Action Plan was not provided.	N/A	The Generator Owner did not perform an analysis of a Misoperation.
PRC-004-1a	R3.	The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its Regional Reliability Organization, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses and its Corrective Action Plans, but did not provide these according to the Regional Reliability Organization's procedures.	N/A	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses but did not provide its Corrective Action Plans.	The responsible entity did not provide its Regional Reliability Organization with documentation of its Misoperations analyses and did not provide its Corrective Action Plans.
PRC-004-2a	R1.	The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		according to the Regional Entity's procedures.				
PRC-004-2a	R2.	The Generator Owner shall analyze its generator Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Entity's procedures.	Documentation of Misoperations is complete, but documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and documentation of Corrective Action Plans is incomplete.	Documentation of Misoperations is incomplete, and there are no associated Corrective Action Plans.	Misoperations have not been analyzed
PRC-004-2a	R3.	The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its Regional Entity, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Entity's procedures.	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses and its Corrective Action Plans, but did not provide these according to the Regional Reliability Organization's procedures.	N/A	The responsible entity provided its Regional Reliability Organization with documentation of its Misoperations analyses but did not provide its Corrective Action Plans.	The responsible entity did not provide its Regional Reliability Organization with documentation of its Misoperations analyses and did not provide its Corrective Action Plans.
PRC-004-WECC-1	R1.	System Operators and System Protection personnel of the Transmission Owners and Generator Owners shall analyze all Protection System and RAS operations.	System Operating personnel of the Transmission Owner or Generator Owner did not review the Protection System Operation or RAS operation within 24 hours but did review the Protection System Operation or RAS operation within six business days.	System Operating personnel of the Transmission Owner or Generator Owner did not review the Protection System operation or RAS operation within six business days.	System Protection personnel of the Transmission Owner and Generator Owner did not analyze the Protection System operation or RAS operation within 20 business days but did analyze the Protection System operation or RAS operation within 25 business days.	System Protection personnel of the Transmission Owner or Generator Owner did not analyze the Protection System operation or RAS operation within 25 business days.
PRC-004-	R1.1.	System Operators shall review all tripping of transmission elements and RAS operations to				

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
WECC-1		identify apparent Misoperations within 24 hours.				
PRC-004-WECC-1	R1.2.	System Protection personnel shall analyze all operations of Protection Systems and RAS within 20 business days for correctness to characterize whether a Misoperation has occurred that may not have been identified by System Operators.				
PRC-004-WECC-1	R2.	Transmission Owners and Generator Owners shall perform the following actions for each Misoperation of the Protection System or RAS. It is not intended that Requirements R2.1 through R2.4 apply to Protection System and/or RAS actions that appear to be entirely reasonable and correct at the time of occurrence and associated system performance is fully compliant with NERC Reliability Standards. If the Transmission Owner or Generator Owner later finds the Protection System or RAS operation to be incorrect through System Protection personnel analysis, the requirements of R2.1 through R2.4 become applicable at the time the Transmission Owner or Generator Owner identifies the Misoperation:				
PRC-004-WECC-1	R2.1.	If the Protection System or RAS has a Security-Based Misoperation and two or more Functionally Equivalent Protection Systems (FEPS) or Functionally Equivalent RAS (FERAS) remain in service to ensure Bulk Electric System (BES) reliability, the Transmission Owners or Generator Owners shall remove from service the Protection System or RAS that misoperated within 22 hours following identification of the Misoperation. Repair or replacement of the failed Protection System or RAS is at the	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 22 hours but did perform the requirements	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 24 hours but did	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 28 hours but did perform the requirements within	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 32 hours.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transmission Owners' and Generator Owners' discretion.	within 24 hours.	perform the requirements within 28 hours.	32 hours.	
PRC-004-WECC-1	R2.2.	If the Protection System or RAS has a Security-Based Misoperation and only one FEPS or FERAS remains in service to ensure BES reliability, the Transmission Owner or Generator Owner shall perform the following.				
PRC-004-WECC-1	R2.2.1.	Following identification of the Protection System or RAS Misoperation, Transmission Owners and Generator Owners shall remove from service within 22 hours for repair or modification the Protection System or RAS that misoperated.	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 22 hours but did perform the requirements within 24 hours.	The Transmission Owner and Generator Owner did not remove from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 24 hours but did perform the requirements within 28 hours.	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 28 hours but did perform the requirements within 32 hours.	The Transmission Owner and Generator Owner did not perform the removal from service, repair, or implement other compliance measures for the Protection System or RAS that misoperated as required within 32 hours.
PRC-004-WECC-1	R2.2.2.	The Transmission Owner or Generator Owner shall repair or replace any Protection System or RAS that misoperated with a FEPS or FERAS within 20 business days of the date of removal. The Transmission Owner or Generator Owner shall remove the Element from service or disable the RAS if repair or replacement is not completed within 20 business days.	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustments to comply with the requirements within 20 business days but did perform the required activities within 25 business days.	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustment to comply with the requirements within 25 business days but did perform the required activities	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustment to comply with the requirements within 28 business days but did perform the required activities within 30 business days.	The Transmission Owner and Generator Owner did not perform the required repairs, replacement, or system operation adjustments to comply with the requirements within 30 business days.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within 28 business days.		
PRC-004-WECC-1	R2.3.	If the Protection System or RAS has a Security-Based or Dependability-Based Misoperation and a FEPS and FERAS is not in service to ensure BES reliability, Transmission Owners or Generator Owners shall repair and place back in service within 22 hours the Protection System or RAS that misoperated. If this cannot be done, then Transmission Owners and Generator Owners shall perform the following.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required within 22 hours but did perform the requirements within 24 hours.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 24 hours but did perform the requirements within 28 hours.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required in less than 28 hours but did perform the requirements within 32 hours.	The Transmission Operator and Generator Owner did not adjust generation to a reliable operating level, adjust the SOL and operate the facilities within established limits or implement other compliance measures for the Protection System or RAS that misoperated as required within 32 hours.
PRC-004-WECC-1	R2.3.1.	When a FEPS is not available, the Transmission Owners shall remove the associated Element from service.				
PRC-004-WECC-1	R2.3.2.	When FERAS is not available, then				
PRC-004-WECC-1	R2.3.2.1.	The Generator Owners shall adjust generation to a reliable operating level, or				
PRC-004-WECC-1	R2.3.2.2.	Transmission Operators shall adjust the SOL and operate the facilities within established limits.				
PRC-004-WECC-1	R2.4.	If the Protection System or RAS has a Dependability-Based Misoperation but has one or more FEPS or FERAS that operated correctly, the associated Element or	The Transmission Owner and Generator Owner did not perform the required	The Transmission Owner and Generator Owner did not perform the	The Transmission Owner and Generator Owner did not perform the required repairs,	The Transmission Owner and Generator Owner did not perform the required

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission path may remain in service without removing from service the Protection System or RAS that failed, provided one of the following is performed.	repairs, replacement, or system operation adjustments to comply with the requirements within 20 business days but did perform the required activities within 25 business days.	required repairs, replacement, or system operation adjustment to comply with the requirements within 25 business days but did perform the required activities within 28 business days.	replacement, or system operation adjustment to comply with the requirements within 28 business days but did perform the required activities within 30 business days.	repairs, replacement, or system operation adjustments to comply with the requirements within 30 business days.
PRC-004-WECC-1	R2.4.1.	Transmission Owners or Generator Owners shall repair or replace any Protection System or RAS that misoperated with FEPS and FERAS within 20 business days of the date of the Misoperation identification, or				
PRC-004-WECC-1	R2.4.2.	Transmission Owners or Generator Owners shall remove from service the associated Element or RAS.				
PRC-004-WECC-1	R3.	Transmission Owners and Generation Owners shall submit Misoperation incident reports to WECC within 10 business days for the following.				
PRC-004-WECC-1	R3.1.	Identification of a Misoperation of a Protection System and/or RAS,	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 10 business days but did perform the required activities within 15 business days.	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 15 business days but did perform the required activities within 20 business days.	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 20 business days but did perform the required activities within 25 business days.	The Transmission Owner and Generator Owner did not report the Misoperation and corrective actions taken or planned to comply with the requirements within 25 business days.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-004-WECC-1	R3.2.	Completion of repairs or the replacement of Protection System and/or RAS that misoperated.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 10 business days of the completion but did perform the required activities within 15 business days.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 15 business days of the completion but did perform the required activities within 20 business days.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 20 business days of the completion but did perform the required activities within 25 business days.	The Transmission Owner and Generator Owner did not report the completion of repair or replacement of Protection System and/or RAS that misoperated to comply with the requirements within 25 business days of the completion.
PRC-005-1b	R1.	Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:	N/A	The responsible entity-had a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES, but the summary of maintenance and testing procedures was missing or incomplete. (R1.2)	The responsible entity had a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES, but the maintenance and testing intervals and their basis were missing or incomplete. (R1.1)	The responsible entity failed to have Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES.
PRC-005-1b	R1.1.	Maintenance and testing intervals and their basis.	N/A	N/A	N/A	N/A
PRC-005-1b	R1.2.	Summary of maintenance and testing procedures.	N/A	N/A	N/A	N/A
PRC-005-1b	R2.	Each Transmission Owner and any Distribution Provider that owns a	The responsible entity provided	Evidence Protection System devices were	Evidence Protection System devices were	Evidence Protection System devices were

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:	documentation of its Protection System maintenance and testing program more than 30 calendar days following a request from its Regional Reliability Organization and/or NERC. OR Evidence Protection System devices were maintained and tested within the defined intervals (R2.1 and R2.2) was missing 5% or less of the applicable devices.	maintained and tested within the defined intervals (R2.1 and R2.2) was missing more than 5% up to (and including) 10% of the applicable devices.	maintained and tested within the defined intervals (R2.1 and R2.2) was missing more than 10% up to (and including) 15% of the applicable devices.	maintained and tested within the defined intervals (R2.1 and R2.2) was missing more than 15% of the applicable devices.
PRC-005-1b	R2.1.	Evidence Protection System devices were maintained and tested within the defined intervals.	N/A	N/A	N/A	N/A
PRC-005-1b	R2.2.	Date each Protection System device was last tested/maintained.	N/A	N/A	N/A	N/A
PRC-006-1	R1.	Each Planning Coordinator shall develop and document criteria, including consideration of historical events and system studies, to select portions of the Bulk Electric System (BES), including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas that may form islands.	N/A	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas	The Planning Coordinator developed and documented criteria but failed to include the consideration of historical events and system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas,	The Planning Coordinator failed to develop and document criteria to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				and Regional Entity areas that may form islands. OR The Planning Coordinator developed and documented criteria but failed to include the consideration of system studies, to select portions of the BES, including interconnected portions of the BES in adjacent Planning Coordinator areas and Regional Entity areas, that may form islands.	that may form islands.	
PRC-006-1	R2.	Each Planning Coordinator shall identify one or more islands to serve as a basis for designing its UFLS program including: *[See Standard pdf for further information]*	N/A	The Planning Coordinator identified an island(s) to serve as a basis for designing its UFLS program but failed to include one (1) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	The Planning Coordinator identified an island(s) to serve as a basis for designing its UFLS program but failed to include two (2) of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3.	The Planning Coordinator identified an island(s) to serve as a basis for designing its UFLS program but failed to include all of the Parts as specified in Requirement R2, Parts 2.1, 2.2, or 2.3. OR The Planning Coordinator failed to identify any island(s) to serve as a basis for designing its UFLS

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						program.
PRC-006-1	R3.	Each Planning Coordinator shall develop a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area, that meets the following performance characteristics in simulations of underfrequency conditions resulting from an imbalance scenario, where an imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s). *[See Standard pdf for further information]*	N/A	The Planning Coordinator developed a UFLS program, including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet one (1) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s)., but failed to meet two (2) of the performance characteristic in Requirement R3, Parts 3.1, 3.2, or 3.3 in simulations of underfrequency conditions.	The Planning Coordinator developed a UFLS program including notification of and a schedule for implementation by UFLS entities within its area where imbalance = [(load — actual generation output) / (load)], of up to 25 percent within the identified island(s).,but failed to meet all the performance characteristic in Requirement R3, Parts 3.1, 3.2, and 3.3 in simulations of underfrequency conditions. OR The Planning Coordinator failed to develop a UFLS program including notification of and a schedule for implementation by UFLS entities within its area
PRC-006-1	R4.	Each Planning Coordinator shall conduct and document a UFLS design assessment at least once every five years that determines	The Planning Coordinator	The Planning Coordinator conducted and	The Planning Coordinator conducted and documented a UFLS	The Planning Coordinator

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2. The simulation shall model each of the following: *[See Standard pdf for further information]*	conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include one (1) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include two (2) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 for each island identified in Requirement R2 but the simulation failed to include three (3) of the items as specified in Requirement R4, Parts 4.1 through 4.7.	conducted and documented a UFLS assessment at least once every five years that determined through dynamic simulation whether the UFLS program design met the performance characteristics in Requirement R3 but simulation failed to include four (4) or more of the items as specified in Requirement R4, Parts 4.1 through 4.7. OR The Planning Coordinator failed to conduct and document a UFLS assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2
PRC-006-1	R5.	Each Planning Coordinator, whose area or portions of whose area is part of an island identified by it or another Planning	N/A	N/A	N/A	The Planning Coordinator, whose area or portions of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Coordinator which includes multiple Planning Coordinator areas or portions of those areas, shall coordinate its UFLS program design with all other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island through one of the following: • Develop a common UFLS program design and schedule for implementation per Requirement R3 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or • Conduct a joint UFLS design assessment per Requirement R4 among the Planning Coordinators whose areas or portions of whose areas are part of the same identified island, or • Conduct an independent UFLS design assessment per Requirement R4 for the identified island, and in the event the UFLS design assessment fails to meet Requirement R3, identify modifications to the UFLS program(s) to meet Requirement R3 and report these modifications as recommendations to the other Planning Coordinators whose areas or portions of whose areas are also part of the same identified island and the ERO.				whose area is part of an island identified by it or another Planning Coordinator which includes multiple Planning Coordinator areas or portions of those areas, failed to coordinate its UFLS program design through one of the manners described in Requirement R5.
PRC-006-1	R6.	Each Planning Coordinator shall maintain a UFLS database containing data necessary to model its UFLS program for use in event analyses and assessments of the UFLS program at least once each calendar year, with no more than 15 months between maintenance activities.	N/A	N/A	N/A	The Planning Coordinator failed to maintain a UFLS database for use in event analyses and assessments of the UFLS program at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						once each calendar year, with no more than 15 months between maintenance activities.
PRC-006-1	R7.	Each Planning Coordinator shall provide its UFLS database containing data necessary to model its UFLS program to other Planning Coordinators within its Interconnection within 30 calendar days of a request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 30 calendar days and up to and including 40 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 40 calendar days but less than and including 50 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 50 calendar days but less than and including 60 calendar days following the request.	The Planning Coordinator provided its UFLS database to other Planning Coordinators more than 60 calendar days following the request. OR The Planning Coordinator failed to provide its UFLS database to other Planning Coordinators.
PRC-006-1	R8.	Each UFLS entity shall provide data to its Planning Coordinator(s) according to the format and schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 5 calendar days but less than or equal to 10 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR	The UFLS entity provided data to its Planning Coordinator(s) more than 10 calendar days but less than or equal to 15 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 15 calendar days but less than or equal to 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.	The UFLS entity provided data to its Planning Coordinator(s) more than 20 calendar days following the schedule specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database. OR The UFLS entity failed to provide data

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The UFLS entity provided data to its Planning Coordinator(s) but the data was not according to the format specified by the Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.		to its Planning Coordinator(s) to support maintenance of each Planning Coordinator's UFLS database.
PRC-006-1	R9.	Each UFLS entity shall provide automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by its Planning Coordinator(s) in each Planning Coordinator area in which it owns assets.	The UFLS entity provided less than 100% but more than (and including) 95% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.	The UFLS entity provided less than 95% but more than (and including) 90% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.	The UFLS entity provided less than 90% but more than (and including) 85% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.	The UFLS entity provided less than 85% of automatic tripping of Load in accordance with the UFLS program design and schedule for application determined by the Planning Coordinator(s) area in which it owns assets.
PRC-006-1	R10.	Each Transmission Owner shall provide automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage as a result of underfrequency load shedding if required by the UFLS program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission.	The Transmission Owner provided less than 100% but more than (and including) 95% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if	The Transmission Owner provided less than 95% but more than (and including) 90% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-	The Transmission Owner provided less than 90% but more than (and including) 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS	The Transmission Owner provided less than 85% automatic switching of its existing capacitor banks, Transmission Lines, and reactors to control over-voltage if required by the UFLS program and schedule

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by the UFLS program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission	voltage if required by the UFLS program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission	program and schedule for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission	for application determined by the Planning Coordinator(s) in each Planning Coordinator area in which the Transmission Owner owns transmission
PRC-006-1	R11.	Each Planning Coordinator, in whose area a BES islanding event results in system frequency excursions below the initializing set points of the UFLS program, shall conduct and document an assessment of the event within one year of event actuation to evaluate: *[See Standard pdf for further information]*	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than one year but less than or equal to 13 months of actuation.	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 13 months but less than or equal to 14 months of actuation.	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 14 months but less than or equal to 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions	The Planning Coordinator, in whose area a BES islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event and evaluated the parts as specified in Requirement R11, Parts 11.1 and 11.2 within a time greater than 15 months of actuation. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate one (1) of the Parts as specified in Requirement R11, Parts11.1 or 11.2.	excursions below the initializing set points of the UFLS program, failed to conduct and document an assessment of the event and evaluate the Parts as specified in Requirement R11, Parts 11.1 and 11.2. OR The Planning Coordinator, in whose area an islanding event resulting in system frequency excursions below the initializing set points of the UFLS program, conducted and documented an assessment of the event within one year of event actuation but failed to evaluate all of the Parts as specified in Requirement R11, Parts 11.1 and 11.2.
PRC-006-1	R12.	Each Planning Coordinator, in whose islanding event assessment (per R11) UFLS program deficiencies are identified, shall conduct and document a UFLS design assessment to consider the identified deficiencies within two years of event actuation.	N/A	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS	The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, conducted and documented a UFLS

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				design assessment to consider the identified deficiencies greater than two years but less than or equal to 25 months of event actuation.	design assessment to consider the identified deficiencies greater than 25 months but less than or equal to 26 months of event actuation.	design assessment to consider the identified deficiencies greater than 26 months of event actuation. OR The Planning Coordinator, in which UFLS program deficiencies were identified per Requirement R11, failed to conduct and document a UFLS design assessment to consider the identified deficiencies.
PRC-006-1	R13.	Each Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, shall coordinate its event assessment (in accordance with Requirement R11) with all other Planning Coordinators whose areas or portions of whose areas were also included in the same islanding event through one of the following: • Conduct a joint event assessment per Requirement R11 among the Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or • Conduct an independent event assessment per Requirement R11 that	N/A	N/A	N/A	The Planning Coordinator, in whose area a BES islanding event occurred that also included the area(s) or portions of area(s) of other Planning Coordinator(s) in the same islanding event and that resulted in system frequency excursions below the initializing set points of the UFLS program, failed to coordinate its UFLS event assessment with all other Planning Coordinators whose

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		reaches conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, or • Conduct an independent event assessment per Requirement R11 and where the assessment fails to reach conclusions and recommendations consistent with those of the event assessments of the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event, identify differences in the assessments that likely resulted in the differences in the conclusions and recommendations and report these differences to the other Planning Coordinators whose areas or portions of whose areas were included in the same islanding event and the ERO.				areas or portions of whose areas were also included in the same islanding event in one of the manners described in Requirement R13
PRC-006-1	R14.	Each Planning Coordinator shall respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the following: *[See Standard pdf for further information]*	N/A	N/A	N/A	The Planning Coordinator failed to respond to written comments submitted by UFLS entities and Transmission Owners within its Planning Coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes were made or reasons why changes were not made to the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						items in Parts 14.1 through 14.3.
PRC-007-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall ensure that its UFLS program is consistent with its Regional Reliability Organization's UFLS program requirements.	The evaluation of the entity's UFLS program for consistency with its Regional Reliability Organization's UFLS program is incomplete or inconsistent in one or more of the Regional Reliability Organization program requirements, but is consistent with the required amount of load shedding.	The amount of load shedding is less than 95 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 90 percent of the Regional requirement in any of the load steps.	The amount of load shedding is less than 85 percent of the Regional requirement in any of the load steps.
PRC-007-0	R2.	The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database.	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database but its annual update was late by 30 calendar days or less.	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database but its annual update was late by more than 30 calendar days but less than or equal to 40 calendar days	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database but its annual update was late by more than 40 calendar days but less than or equal to 50 calendar days.	The responsible entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) did not provided its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLS program database, OR The responsible entity's annual update was late by more than 50 calendar days.

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-007-0	R3.	The Transmission Owner and Distribution Provider that owns a UFLS program (as required by its Regional Reliability Organization) shall provide its documentation of that UFLS program to its Regional Reliability Organization on request (30 calendar days).	The responsible entity has provided the documentation in more than 30 calendar days but less than or equal to 40 calendar days.	The responsible entity has provided the documentation in more than 40 calendar days but less than or equal to 50 calendar days.	The responsible entity has provided the documentation in more than 50 calendar days but less than or equal to 60 calendar days.	The responsible entity has not provided the documentation for more than 60 calendar days.
PRC-008-0	R1.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall have a UFLS equipment maintenance and testing program in place. This UFLS equipment maintenance and testing program shall include UFLS equipment identification, the schedule for UFLS equipment testing, and the schedule for UFLS equipment maintenance.	The UFLS equipment identification, testing schedule or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing 5% or less of the applicable equipment.	The UFLS equipment identification, testing schedule, or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing for more than 5% up to (and including) 10% of the applicable equipment.	The UFLS equipment identification, testing schedule, or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing more than 10% up to (and including) 15% of the applicable equipment.	The responsible entity failed to implement UFLS equipment maintenance and testing program. OR The UFLS equipment identification, testing schedule, or maintenance schedule for the responsible entity's UFLS equipment maintenance and testing program was missing more than 15% of the applicable equipment.
PRC-008-0	R2.	The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UFLS equipment maintenance and testing program more than 30 calendar days following a request from its Regional Reliability Organization and/or NERC.	Evidence UFLS equipment was maintained and tested within the defined intervals was missing for more than 5% up to (and including) 10% of the applicable devices.	Evidence UFLS equipment was maintained and tested within the defined intervals was missing for more than 10% up to (and including) 15% of the applicable devices.	Evidence UFLS equipment was maintained and tested within the defined intervals was missing for more than 15% of the applicable devices.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR Evidence UFLS equipment was maintained and tested within the defined intervals was missing for 5% or less of the applicable devices.			
PRC-009-0	R1.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:	The responsible entity that owns or operates a UFLS program failed to include one of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.	The responsible entity that owns or operates a UFLS program failed to include two of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.	The responsible entity that owns or operates a UFLS program failed to include three of the elements listed in PRC-009-0 R1.1 through R1.4 in the analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.	The responsible entity that owns or operates a UFLS program failed to conduct an analysis of the performance of UFLS equipment and Program effectiveness, as described in PRC-009-0 R1, following system events resulting in system frequency excursions below the initializing set points of the UFLS program.
PRC-009-0	R1.1.	A description of the event including initiating conditions.	N/A	N/A	N/A	N/A
PRC-009-0	R1.2.	A review of the UFLS set points and tripping times.	N/A	N/A	N/A	N/A
PRC-009-0	R1.3.	A simulation of the event.	N/A	N/A	N/A	N/A
PRC-009-0	R1.4.	A summary of the findings.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-009-0	R2.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.	The responsible entity has provided the documentation in more than 90 calendar days but less than 105 calendar days.	The responsible entity has provided the documentation in more than 105 calendar days but less than 129 calendar days.	The responsible entity has provided the documentation in more than 129 calendar days but less than 145 calendar days.	The responsible entity has provided the documentation in 145 calendar days or more.
PRC-010-0	R1.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).	The responsible entity conducted an assessment of the effectiveness of its UVLS system within 5 years or as required by changes in system conditions but did not include the associated Transmission Planner(s) and Planning Authority(ies).	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 5 years but did in less than or equal to 6 years. OR The assessment of the effectiveness of the responsible entity's UVLS system did not address one of the elements in R1 (R1.1.1 through R1.1.3).	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 6 years but did in less than or equal to 7years. OR The assessment of the effectiveness of the responsible entity's UVLS system did not address two of the elements in R1 (R1.1.1 through R1.1.3).	The responsible entity did not conduct an assessment of the effectiveness of its UVLS system for more than 7 years. OR The assessment of the effectiveness of the responsible entity's UVLS system did not address any of the elements in R1 (R1.1.1 through R1.1.3).
PRC-010-0	R1.1.	This assessment shall include, but is not limited to:	N/A	N/A	N/A	N/A
PRC-010-0	R1.1.1.	Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-010-0	R1.1.2.	Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.	N/A	N/A	N/A	N/A
PRC-010-0	R1.1.3.	A review of the voltage set points and timing.	N/A	N/A	N/A	N/A
PRC-010-0	R2. (Retired)	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).	The responsible entity provided documentation of its current UVLS program assessment more than 30 calendar but less than or equal to 40 calendar days following a request from its Regional Reliability Organization or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 40 calendar days but less than or equal to 50 calendar days following a request from its Regional Reliability Organization or NERC.	The responsible entity provided documentation of its current UVLS program assessment more than 50 calendar days but less than or equal to 60 calendar days following a request from its Regional Reliability Organization or NERC.	The responsible entity did not provide documentation of its current UVLS program assessment for more than 60 calendar days following a request from its Regional Reliability Organization or NERC.
PRC-011-0	R1.	The Transmission Owner and Distribution Provider that owns a UVLS system shall have a UVLS equipment maintenance and testing program in place. This program shall include:	The responsible entity's UVLS equipment maintenance and testing program did not address one of the subrequirements in R1.2 through R1.6. OR The responsible entity's UVLS program did not address one of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's UVLS equipment maintenance and testing program did not address two of the subrequirements in R1.2 through R1.6. OR The responsible entity's UVLS program did not address two of the equipment classes as specified in R1.1.1	The responsible entity's UVLS equipment maintenance and testing program did not address three of the subrequirements in R1.1 through R1.6. OR The responsible entity's UVLS program did not address three of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's UVLS equipment maintenance and testing program did not address four or more of the subrequirements in R1.2 through R1.6. OR The responsible entity's UVLS program did not address any of the equipment classes as specified in R1.1.1

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				through R1.1.4.		through R1.1.4.
PRC-011-0	R1.1.	The UVLS system identification which shall include but is not limited to:	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.1.	Relays.	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.2.	Instrument transformers.	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.3.	Communications systems, where appropriate.	N/A	N/A	N/A	N/A
PRC-011-0	R1.1.4.	Batteries.	N/A	N/A	N/A	N/A
PRC-011-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	N/A	N/A	N/A	N/A
PRC-011-0	R1.3.	Summary of testing procedure.	N/A	N/A	N/A	N/A
PRC-011-0	R1.4.	Schedule for system testing.	N/A	N/A	N/A	N/A
PRC-011-0	R1.5.	Schedule for system maintenance.	N/A	N/A	N/A	N/A
PRC-011-0	R1.6.	Date last tested/maintained.	N/A	N/A	N/A	N/A
PRC-011-0	R2.	The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was missing	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was	The responsible entity provided documentation of its UVLS equipment maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was missing for more than 10% up to (and including) 15% of the applicable devices.	The responsible entity did not provide documentation of its UVLS equipment maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC. OR Evidence UVLS equipment was maintained and tested within the defined intervals was missing for more than 15% of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			for 5% or less of the applicable devices.	missing for more than 5% up to (and including) 10% of the applicable devices.		the applicable devices.
PRC-015-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall maintain a list of and provide data for existing and proposed SPSs as specified in Reliability Standard PRC-013-0_R 1.	N/A	The responsible entity's list of existing or proposed SPSs did not address one of the subrequirements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.	The responsible entity's list of existing or proposed SPSs did not address two of the subrequirements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.	The responsible entity's list of existing or proposed SPSs did not address any of the subrequirements in R1.1 through R1.3 as specified in Reliability Standard PRC-013-0_R1.
PRC-015-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have evidence it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures as defined in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address one of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address two of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address three of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.	The responsible entity was not compliant in that evidence that it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures did not address four or more of the subrequirements in R1.1 through R1.9 as specified in Reliability Standard PRC-012-0_R1 prior to being placed in service.
PRC-015-0	R3.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and	The responsible entity provided documentation of its	The responsible entity provided documentation of its	The responsible entity provided documentation of its SPS data and the	The responsible entity provided documentation of its

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the results of studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).	SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 30 calendar days but less than or equal to 40 calendar days following a request from its Regional Reliability Organization or NERC.	SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 40 calendar days but less than or equal to 50 calendar days following a request from its Regional Reliability Organization or NERC.	results of the studies that show compliance of new or functionally modified SPSs more than 50 calendar days but less than or equal to 60 calendar days following a request from its Regional Reliability Organization or NERC.	SPS data and the results of the studies that show compliance of new or functionally modified SPSs more than 60 calendar days following a request from its Regional Reliability Organization or NERC.
PRC-016-0.1	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall analyze its SPS operations and maintain a record of all misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R 1.	N/A	N/A	N/A	The responsible entity that owns an SPS did not analyze its SPS operations and maintain a record of all Misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R 1.
PRC-016-0.1	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall take corrective actions to avoid future misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take 5% or less of the corrective actions designed to avoid future SPS Misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take more than 5% up to (and including) 10% of the corrective actions designed to avoid future SPS Misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take more than 10% up to (and including) 15% of the corrective actions designed to avoid future SPS Misoperations.	For each Misoperation, the responsible entity that owns an SPS did not take more than 15% of the corrective actions designed to avoid future SPS Misoperations.
PRC-016-	R3.	The Transmission Owner, Generator Owner,	The responsible entity	The responsible	The responsible entity	The responsible entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
0.1		and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).	provided documentation of its SPS Misoperation analyses and the corrective action plans more than 90 calendar days but less than or equal to 120 calendar days following a request from its Regional Reliability Organization or NERC.	entity provided documentation of its SPS Misoperation analyses and the corrective action plans more than 120 calendar days but less than or equal to 130 calendar days following a request from its Regional Reliability Organization or NERC.	provided documentation of its SPS Misoperation analyses and the corrective action plans more than 130 calendar days but less than or equal to140 calendar days following a request from its Regional Reliability Organization or NERC.	provided documentation of its SPS Misoperation analyses and the corrective action plans more than 140 calendar days following a request from its Regional Reliability Organization or NERC. OR Did not provide the documentation.
PRC-017-0	R1.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have a system maintenance and testing program(s) in place. The program(s) shall include:	The responsible entity's SPS equipment maintenance and testing program did not address one of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address one of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's SPS equipment maintenance and testing program did not address two of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address two of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's SPS equipment maintenance and testing program did not address three of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address three of the equipment classes as specified in R1.1.1 through R1.1.4.	The responsible entity's SPS equipment maintenance and testing program did not address four or more of the subrequirements in R1.2 through R1.6. OR The responsible entity's SPS program did not address any of the equipment classes as specified in R1.1.1 through R1.1.4.
PRC-017-0	R1.1.	SPS identification shall include but is not limited to:	N/A	N/A	N/A	N/A
PRC-017-0	R1.1.1.	Relays.	N/A	N/A	N/A	N/A
PRC-017-0	R1.1.2.	Instrument transformers.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-017-0	R1.1.3.	Communications systems, where appropriate.	N/A	N/A	N/A	N/A
PRC-017-0	R1.1.4.	Batteries.	N/A	N/A	N/A	N/A
PRC-017-0	R1.2.	Documentation of maintenance and testing intervals and their basis.	N/A	N/A	N/A	N/A
PRC-017-0	R1.3.	Summary of testing procedure.	N/A	N/A	N/A	N/A
PRC-017-0	R1.4.	Schedule for system testing.	N/A	N/A	N/A	N/A
PRC-017-0	R1.5.	Schedule for system maintenance.	N/A	N/A	N/A	N/A
PRC-017-0	R1.6.	Date last tested/maintained.	N/A	N/A	N/A	N/A
PRC-017-0	R2.	The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days).	The responsible entity provided documentation of its SPS maintenance and testing program more than 30 but less than or equal to 40 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 40 but less than or equal to 50 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity provided documentation of its SPS maintenance and testing program more than 50 but less than or equal to 60 days following a request from its Regional Reliability Organization and/or NERC.	The responsible entity did not provide documentation of its SPS maintenance and testing program for more than 60 days following a request from its Regional Reliability Organization and/or NERC.
PRC-018-1	R1.	Each Transmission Owner and Generator Owner required to install DMEs by its Regional Reliability Organization (reliability standard PRC-002 Requirements 1-3) shall have DMEs installed that meet the following requirements:	N/A	N/A	The installation of DMEs does not include one of the subrequirements in R1.1 and R1.2.	The installation of DMEs does not include any of the subrequirements in R1.1 and R1.2.
PRC-018-1	R1.1.	Internal Clocks in DME devices shall be synchronized to within 2 milliseconds or less of Universal Coordinated Time scale (UTC)	N/A	N/A	N/A	N/A
PRC-018-1	R1.2.	Recorded data from each Disturbance shall be retrievable for ten calendar days.	N/A	N/A	N/A	N/A
PRC-018-1	R2.	The Transmission Owner and Generator Owner shall each install DMEs in	The responsible entity failed to install 5% or	The responsible entity failed to	The responsible entity failed to install more	The responsible entity failed to install more

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		accordance with its Regional Reliability Organization's installation requirements (reliability standard PRC-002 Requirements 1 through 3).	less of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.	install more than 5% up to (and including) 10% of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.	than 10% up to (and including) 15% of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.	than 15% of the DME devices in accordance with its Regional Reliability Organization's installation requirements as defined in PRC-002 R1 through R3.
PRC-018-1	R3.	The Transmission Owner and Generator Owner shall each maintain, and report to its Regional Reliability Organization on request, the following data on the DMEs installed to meet that region's installation requirements (reliability standard PRC-002 Requirements1.1, 2.1 and 3.1):	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for one of the subrequirements in R3.1 through R3.8.	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for two of the subrequirements in R3.1 through R3.8.	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for three of the subrequirements in R3.1 through R3.8.	Evidence that the responsible entity maintained data on the DMEs installed to meet that region's installation requirements was missing or not reported for four or more of the subrequirements in R3.1 through R3.8.
PRC-018-1	R3.1.	Type of DME (sequence of event recorder, fault recorder, or dynamic disturbance recorder).	N/A	N/A	N/A	N/A
PRC-018-1	R3.2.	Make and model of equipment.	N/A	N/A	N/A	N/A
PRC-018-1	R3.3.	Installation location.	N/A	N/A	N/A	N/A
PRC-018-1	R3.4.	Operational status.	N/A	N/A	N/A	N/A
PRC-018-1	R3.5.	Date last tested.	N/A	N/A	N/A	N/A
PRC-018-1	R3.6.	Monitored elements, such as transmission circuit, bus section, etc.	N/A	N/A	N/A	N/A
PRC-018-1	R3.7.	Monitored devices, such as circuit breaker, disconnect status, alarms, etc.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-018-1	R3.8.	Monitored electrical quantities, such as voltage, current, etc.	N/A	N/A	N/A	N/A
PRC-018-1	R4.	The Transmission Owner and Generator Owner shall each provide Disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements (reliability standard PRC-002 Requirement 4).	The responsible entity did not provide 5% or less of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity did not provide more than 5% up to (and including) 10% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity did not provide more than 10% up to (and including) 15% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.	The responsible entity did not provide more than 15% of the disturbance data (recorded by DMEs) in accordance with its Regional Reliability Organization's requirements.
PRC-018-1	R5.	The Transmission Owner and Generator Owner shall each archive all data recorded by DMEs for Regional Reliability Organization-identified events for at least three years.	5% or less of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.	More than 5% up to (and including) 10% of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.	More than 10% up to (and including) 15% of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.	More than 15% of the responsible entity's data recorded by DMEs for Regional Reliability Organization-identified events was not archived for at least three years.
PRC-018-1	R6.	Each Transmission Owner and Generator Owner that is required by its Regional Reliability Organization to have DMEs shall have a maintenance and testing program for those DMEs that includes:	N/A	N/A	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include one of the elements in R6.1 and 6.2.	The responsible entity is not compliant in that the maintenance and testing program for DMEs does not include any of the elements in R6.1 and 6.2.
PRC-018-1	R6.1.	Maintenance and testing intervals and their basis.	The responsible entity's DME maintenance and testing program was	The responsible entity's DME maintenance and testing program was	The responsible entity's DME maintenance and testing program was non-compliant in that	The responsible entity's DME maintenance and testing program was

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			non-compliant in that documentation of maintenance and testing intervals and their basis was missing for no more than 25% of the DME equipment.	non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 25% but less than or equal to 50% of the DME equipment.	documentation of maintenance and testing intervals and their basis was missing for more than 50% but less than or equal to 75% of the DME equipment.	non-compliant in that documentation of maintenance and testing intervals and their basis was missing for more than 75% of the DME equipment.
PRC-018-1	R6.2.	Summary of maintenance and testing procedures.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for no more than 25% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for more than 25% but less than or equal to 50% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for more than 50% but less than or equal to 75% of the DME equipment.	The responsible entity's DME maintenance and testing program was non-compliant in that the summary of maintenance and testing procedures documentation was missing for more than 75% of the DME equipment.
PRC-021-1	R1.	Each Transmission Owner and Distribution Provider that owns a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall annually update its UVLS data to support the Regional UVLS program database. The following data shall be provided to the Regional Reliability Organization for each installed UVLS system:	UVLS data was provided but did not address one of the subrequirements in R1.1 through R1.5.	UVLS data was provided but did not address two of the subrequirements in R1.1 through R1.5.	UVLS data was provided but did not address three of the subrequirements in R1.1 through R1.5.	No annual UVLS data was provided. OR UVLS data was provided but did not address four or more of the subrequirements in R1.1 through R1.5.
PRC-021-1	R1.1.	Size and location of customer load, or percent of connected load, to be interrupted.	N/A	N/A	N/A	N/A
PRC-021-1	R1.2.	Corresponding voltage set points and overall	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		scheme clearing times.				
PRC-021-1	R1.3.	Time delay from initiation to trip signal.	N/A	N/A	N/A	N/A
PRC-021-1	R1.4.	Breaker operating times.	N/A	N/A	N/A	N/A
PRC-021-1	R1.5.	Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.	N/A	N/A	N/A	N/A
PRC-021-1	R2.	Each Transmission Owner and Distribution Provider that owns a UVLS program shall provide its UVLS program data to the Regional Reliability Organization within 30 calendar days of a request.	The responsible entity updated its UVLS data more than 30 calendar days but less than or equal to 40 calendar days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 40 calendar days but less than or equal to 50 calendar days following a request from its Regional Reliability Organization.	The responsible entity updated its UVLS data more than 50 calendar days but less than or equal to 60 calendar days following a request from its Regional Reliability Organization.	The responsible entity did not update its UVLS data for more than 60 calendar days following a request from its Regional Reliability Organization.
PRC-022-1	R1.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:	The overall analysis program did not address one of the subrequirements in R1.1 through R1.5.	The overall analysis program did not address two of the subrequirements in R1.1 through R1.5.	The overall analysis program did not address three of the subrequirements in R1.1 through R1.5.	The responsible entity failed to analyze and document a UVLS operation and Misoperation. OR The overall analysis program did not address four or more of the subrequirements in R1.1 through R1.5.
PRC-022-1	R1.1.	A description of the event including initiating conditions.	N/A	N/A	N/A	N/A
PRC-022-1	R1.2.	A review of the UVLS set points and tripping times.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-022-1	R1.3.	A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.	N/A	N/A	N/A	N/A
PRC-022-1	R1.4.	A summary of the findings.	N/A	N/A	N/A	N/A
PRC-022-1	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.	N/A	N/A	N/A	N/A
PRC-022-1	R2. (Retired)	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.	The responsible entity provided documentation of the analysis of UVLS program performance more than 90 calendar days but less than or equal to 120 calendar days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 120 calendar days but less than or equal to 130 calendar days following a request from its Regional Reliability Organization.	The responsible entity provided documentation of the analysis of UVLS program performance more than 130 calendar days but less than or equal to 140 calendar days following a request from its Regional Reliability Organization.	The responsible entity did not provide documentation of the analysis of UVLS program performance for more than 140 calendar days following a request from its Regional Reliability Organization.
PRC-023-1	R1.	Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (R1.1 through R1.13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the Bulk Electric System for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees: [Mitigation Time Horizon: Long		Evidence that relay settings comply with criteria in R1.1 though 1.13 exists, but evidence is incomplete or incorrect for one or more of the subrequirements.		Relay settings do not comply with any of the sub requirements R1.1 through R1.13 OR Evidence does not exist to support that relay settings comply with one of the criteria in subrequirements R1.1 through R1.13.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Term Planning].				
PRC-023-1	R2.	The Transmission Owner, Generator Owner, or Distribution Provider that uses a circuit capability with the practical limitations described in R1.6, R1.7, R1.8, R1.9, R1.12, or R1.13 shall use the calculated circuit capability as the Facility Rating of the circuit and shall obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability. [Time Horizon: Long Term Planning]	Criteria described in R1.6, R1.7. R1.8. R1.9, R1.12, or R.13 was used but evidence does not exist that agreement was obtained in accordance with R2.			
PRC-023-1	R3.	The Planning Coordinator shall determine which of the facilities (transmission lines operated at 100 kV to 200 kV and transformers with low voltage terminals connected at 100 kV to 200 kV) in its Planning Coordinator Area are critical to the reliability of the Bulk Electric System to identify the facilities from 100 kV to 200 kV that must meet Requirement 1 to prevent potential cascade tripping that may occur when protective relay settings limit transmission loadability. [Time Horizon: Long Term Planning]		Provided the list of facilities critical to the reliability of the Bulk Electric System to the appropriate Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers between 31 days and 45 days after the list was established or updated.	Provided the list of facilities critical to the reliability of the Bulk Electric System to the appropriate Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers between 46 days and 60 days after list was established or updated.	Does not have a process in place to determine facilities that are critical to the reliability of the Bulk Electric System. OR Does not maintain a current list of facilities critical to the reliability of the Bulk Electric System, OR Did not provide the list of facilities critical to the reliability of the Bulk Electric System to the appropriate Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers, or provided the list more than 60

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						days after the list was established or updated.
PRC-023-2	R1	Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (Requirement R1, criteria 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the BES for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees. [See Standard for Criteria]	N/A	N/A	N/A	The responsible entity did not use any one of the following criteria (Requirement R1 criterion 1 through 13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the Bulk Electric System for all fault conditions. OR The responsible entity did not evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees.
PRC-023-2	R2	Each Transmission Owner, Generator Owner, and Distribution Provider shall set its out-of-step blocking elements to allow tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1.	N/A	N/A	N/A	The responsible entity failed to ensure that its out-of-step blocking elements allowed tripping of phase protective relays for faults that occur during the loading conditions used to verify transmission line relay loadability per Requirement R1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
PRC-023-2	R3	Each Transmission Owner, Generator Owner, and Distribution Provider that uses a circuit capability with the practical limitations described in Requirement R1, criterion 6, 7, 8, 9, 12, or 13 shall use the calculated circuit capability as the Facility Rating of the circuit and shall obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability.	N/A	N/A	N/A	The responsible entity that uses a circuit capability with the practical limitations described in Requirement R1 criterion 6, 7, 8, 9, 12, or 13 did not use the calculated circuit capability as the Facility Rating of the circuit. OR The responsible entity did not obtain the agreement of the Planning Coordinator, Transmission Operator, and Reliability Coordinator with the calculated circuit capability.
PRC-023-2	R4	Each Transmission Owner, Generator Owner, and Distribution Provider that chooses to use Requirement R1 criterion 2 as the basis for verifying transmission line relay loadability shall provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits associated with those transmission line relays at least once each calendar year, with no more than 15 months between reports.	N/A	N/A	N/A	The responsible entity did not provide its Planning Coordinator, Transmission Operator, and Reliability Coordinator with an updated list of circuits that have transmission line relays set according to the criteria established in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1 criterion 2 at least once each calendar year, with no more than 15 months between reports.
PRC-023-2	R5	Each Transmission Owner, Generator Owner, and Distribution Provider that sets transmission line relays according to Requirement R1 criterion 12 shall provide an updated list of the circuits associated with those relays to its Regional Entity at least once each calendar year, with no more than 15 months between reports, to allow the ERO to compile a list of all circuits that have protective relay settings that limit circuit capability.	N/A	N/A	N/A	The responsible entity did not provide its Regional Entity, with an updated list of circuits that have transmission line relays set according to the criteria established in Requirement R1 criterion 12 at least once each calendar year, with no more than 15 months between reports.
PRC-023-2	R6	Each Planning Coordinator shall conduct an assessment at least once each calendar year, with no more than 15 months between assessments, by applying the criteria in Attachment B to determine the circuits in its Planning Coordinator area for which Transmission Owners, Generator Owners, and Distribution Providers must comply with Requirements R1 through R5. The Planning Coordinator shall: *[See standard for what the Planning Coordinator shall do]*	N/A	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but more than 15 months and less than 24 months lapsed between	The Planning Coordinator used the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met parts 6.1 and 6.2, but 24 months or more lapsed between assessments. OR The Planning	The Planning Coordinator failed to use the criteria established within Attachment B to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard. OR The Planning Coordinator used the criteria established

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but failed to include the calendar year in which any criterion in Attachment B first applies. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the	Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 46 days and 60 days after list was established or updated. (part 6.2)	within Attachment B, at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to meet parts 6.1 and 6.2. OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard but failed to maintain the list of circuits determined according to the process described in Requirement R6. (part 6.1)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 and 6.2 but provided the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area between 31 days and 45 days after the list was established or updated. (part 6.2)		OR The Planning Coordinator used the criteria established within Attachment B at least once each calendar year, with no more than 15 months between assessments to determine the circuits in its Planning Coordinator area for which applicable entities must comply with the standard and met 6.1 but failed to provide the list of circuits to the Reliability Coordinators, Transmission Owners, Generator Owners, and Distribution Providers within its Planning Coordinator area or provided the list more than 60 days after the list was established or updated. (part 6.2) OR The Planning Coordinator failed to determine the circuits in its Planning Coordinator area for

Complete Violation Severity Level Matrix (PRC)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						which applicable entities must comply with the standard.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-001-1a	R1.	Each Transmission Operator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area and shall exercise specific authority to alleviate operating emergencies.	N/A	N/A	N/A	The Transmission Operator has no evidence that clear decision-making authority exists to assure reliability in its area or has failed to exercise this authority to alleviate operating emergencies.
TOP-001-1a	R2.	Each Transmission Operator shall take immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.	N/A	N/A	N/A	The Transmission Operator failed to have evidence that it took immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.
TOP-001-1a	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the	N/A	N/A	N/A	The responsible entity failed to comply with reliability directives issued by the Reliability Coordinator or the Transmission Operator (when applicable), when said directives would not have resulted in actions that would violate safety,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.				equipment, regulatory or statutory requirements, or under circumstances that said directives would have resulted in actions that would violate safety, equipment, regulatory or statutory requirements the responsible entity failed to inform the Reliability Coordinator or Transmission Operator (when applicable) of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator could implement alternate remedial actions.
TOP-001-1a	R4.	Each Distribution Provider and Load-Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions.	N/A	N/A	N/A	The responsible entity failed to comply with all reliability directives issued by the Transmission Operator, including shedding firm load, when said directives would not have resulted in actions that would violate safety, equipment, regulatory or statutory requirements, or under

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						circumstances when said directives would have violated safety, equipment, regulatory or statutory requirements, the responsible entity failed to immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator could implement alternate remedial actions.
TOP-001-1a	R5.	Each Transmission Operator shall inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, and take actions to avoid, when possible, or mitigate the emergency.	N/A	The Transmission Operator failed to inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, but did take actions to avoid, when possible, or mitigate the emergency.	N/A	The Transmission Operator failed to inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, and failed to take actions to avoid, when possible, or mitigate the emergency.
TOP-001-1a	R6.	Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.	N/A	N/A	N/A	The responsible entity failed to render all available emergency assistance to others as requested, after the requesting entity had implemented its comparable

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						emergency procedures, when said assistance would not have resulted in actions that would violate safety, equipment, or regulatory or statutory requirements.
TOP-001-1a	R7.	Each Transmission Operator and Generator Operator shall not remove Bulk Electric System facilities from service if removing those facilities would burden neighboring systems unless:	N/A	N/A	N/A	The responsible entity removed Bulk Electric System facilities from service and removal of said facilities burdened a neighboring system, without complying with the applicable requirements listed in R7.1 through R7.3.
TOP-001-1a	R7.1.	For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	N/A
TOP-001-1a	R7.2.	For a transmission facility, the Transmission Operator shall notify and coordinate with its Reliability Coordinator. The Transmission Operator shall notify other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	N/A	N/A	N/A	N/A
TOP-001-1a	R7.3.	When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public,	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.				
TOP-001-1a	R8.	During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.	N/A	N/A	N/A	The responsible entity failed to take immediate actions to restore the Real and Reactive Power Balance during a system emergency. OR The responsible entity failed to request emergency assistance from the Reliability Coordinator during a period when it was unable to restore the Real and Reactive Power Balance, OR During a period when corrective actions or emergency assistance was not adequate to mitigate the Real and Reactive Power Balance, the responsible entity failed to implement firm load shedding.
TOP-002-2.1b	R1.	Each Balancing Authority and Transmission Operator shall maintain a set of current plans	N/A	N/A	The responsible entity maintained a set of	The responsible entity failed to maintain a set

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that are designed to evaluate options and set procedures for reliable operation through a reasonable future time period. In addition, each Balancing Authority and Transmission Operator shall be responsible for using available personnel and system equipment to implement these plans to ensure that interconnected system reliability will be maintained.			current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period, but failed to utilize available personnel and system equipment to implement these plans to ensure that interconnected system reliability would be maintained.	of current plans that were designed to evaluate options and set procedures for reliable operation through a reasonable future time period.
TOP-002-2.1b	R2.	Each Balancing Authority and Transmission Operator shall ensure its operating personnel participate in the system planning and design study processes, so that these studies contain the operating personnel perspective and system operating personnel are aware of the planning purpose.	N/A	N/A	N/A	The responsible entity failed to ensure its operating personnel participated in the system planning and design study processes.
TOP-002-2.1b	R3.	Each Load-Serving Entity and Generator Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider. Each Balancing Authority and Transmission Service Provider shall coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed to coordinate its seasonal	N/A	The Load-Serving Entity or Generator Operator failed to coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider, or the Balancing Authority or Transmission Service Provider failed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				operations with its Transmission Operator.		to coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.
TOP-002-2.1b	R4.	Each Balancing Authority and Transmission Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator, so that normal Interconnection operation will proceed in an orderly and consistent manner.	N/A	The responsible entity failed to coordinate (where confidentiality agreements allow) one of the following three categories of operations (current-day, next-day or seasonal) with the applicable entity(ies)	The responsible entity failed to coordinate (where confidentiality agreements allow) two of the following three categories of operations (current-day, next-day or seasonal) with the applicable entity(ies)	The responsible entity failed to coordinate (where confidentiality agreements allow) all three of the following categories of operations (current-day, next-day or seasonal) with the applicable entity(ies)
TOP-002-2.1b	R5.	Each Balancing Authority and Transmission Operator shall plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.	N/A	N/A	N/A	The responsible entity failed to plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.
TOP-002-2.1b	R6.	Each Balancing Authority and Transmission Operator shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional, and local reliability requirements.	N/A	N/A	N/A	The responsible entity failed to plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional and local reliability

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						requirements.
TOP-002-2.1b	R7.	Each Balancing Authority shall plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet capacity and energy reserve requirements, including the deliverability/capability for any single Contingency.
TOP-002-2.1b	R8.	Each Balancing Authority shall plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet voltage and/or reactive limits, including the deliverability/capability for any single contingency.
TOP-002-2.1b	R9.	Each Balancing Authority shall plan to meet Interchange Schedules and Ramps.	N/A	N/A	N/A	The Balancing Authority failed to plan to meet Interchange Schedules and Ramps.
TOP-002-2.1b	R10.	Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).	N/A	N/A	N/A	The responsible entity failed to plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).
TOP-002-2.1b	R11.	The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs. Neighboring Transmission Operators shall utilize identical SOLs for common facilities. The Transmission Operator shall update	N/A	N/A	The Transmission Operator performed seasonal, next-day, and current-day Bulk Electric System studies, reflecting	The Transmission Operator failed to perform seasonal, next-day, or current-day Bulk Electric System studies,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject confidentiality requirements), and to its Reliability Coordinator.			current system conditions, to determine SOLs, but failed to make the results of Bulk Electric System studies available to all of the Transmission Operators, Balancing Authorities (subject confidentiality requirements), or to its Reliability Coordinator.	reflecting current system conditions, to determine SOLs.
TOP-002-2.1b	R12.	The Transmission Service Provider shall include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available Transfer Capability calculation processes.	N/A	N/A	N/A	The Transmission Service Provider failed to include known SOLs or IROLs within its area and neighboring areas in the determination of transfer capabilities, in accordance with filed tariffs and/or regional Total Transfer Capability and Available Transfer Capability calculation processes.
TOP-002-2.1b	R13.	At the request of the Balancing Authority or Transmission Operator, a Generator Operator shall perform generating real and reactive capability verification that shall include, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, and provide the results to the Balancing Authority or Transmission Operator operating personnel as requested.	N/A	N/A	N/A	The Generator Operator failed to perform generating real and reactive capability verification that included, among other variables, weather, ambient air and water conditions,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						and fuel quality and quantity, or failed to provide the results of generating real and reactive verifications Balancing Authority or Transmission Operator operating personnel, when requested.
TOP-002-2.1b	R14.	Generator Operators shall, without any intentional time delay, notify their Balancing Authority and Transmission Operator of changes in capabilities and characteristics including but not limited to:	N/A	N/A	N/A	The Generator Operator failed to notify its Balancing Authority or Transmission Operator of changes in capabilities and characteristics including real output capabilities.
TOP-002-2.1b	R14.1.	Changes in real output capabilities.	N/A	N/A	N/A	N/A
TOP-002-2.1b	R15.	Generation Operators shall, at the request of the Balancing Authority or Transmission Operator, provide a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).	N/A	N/A	N/A	The Generator Operator failed to provide, at the request of the Balancing Authority or Transmission Operator, a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).
TOP-002-2.1b	R16.	Subject to standards of conduct and confidentiality agreements, Transmission	N/A	N/A	N/A	The Transmission Operator failed to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Operators shall, without any intentional time delay, notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics including but not limited to:				notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2.1b	R16.1.	Changes in transmission facility status.	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility status, within the terms and conditions of standards of conduct and confidentiality agreements.
TOP-002-2.1b	R16.2.	Changes in transmission facility rating.	N/A	N/A	N/A	The Transmission Operator failed to notify their Reliability Coordinator and Balancing Authority of changes in transmission facility rating, within the terms and conditions of standards of conduct and confidentiality agreements.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TOP-002-2.1b	R17.	Balancing Authorities and Transmission Operators shall, without any intentional time delay, communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.	N/A	N/A	N/A	The responsible entity failed to communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.
TOP-002-2.1b	R18.	Neighboring Balancing Authorities, Transmission Operators, Generator Operators, Transmission Service Providers, and Load-Serving Entities shall use uniform line identifiers when referring to transmission facilities of an interconnected network.	N/A	N/A	N/A	The responsible entity failed to use uniform line identifiers when referring to transmission facilities of an interconnected network.
TOP-002-2.1b	R19.	Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations.	N/A	N/A	N/A	The responsible entity failed to maintain accurate computer models utilized for analyzing and planning system operations.
TOP-004-2	R1.	Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).	N/A	N/A	N/A	The Transmission Operator failed to operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).
TOP-004-2	R2.	Each Transmission Operator shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.	N/A	N/A	N/A	The Transmission Operator failed to operate so that instability, uncontrolled separation, or cascading outages

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						would not occur as a result of the most severe single contingency.
TOP-004-2	R3.	Each Transmission Operator shall operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by its Reliability Coordinator.	N/A	N/A	N/A	The Transmission Operator failed to operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by Reliability Coordinator policy.
TOP-004-2	R4.	If a Transmission Operator enters an unknown operating state (i.e., any state for which valid operating limits have not been determined), it will be considered to be in an emergency and shall restore operations to respect proven reliable power system limits within 30 minutes.	N/A	N/A	N/A	The Transmission Operator entered an unknown operating state (i.e., any state for which valid operating limits have not been determined), and failed to restore operations to respect proven reliable power system limits for more than 30 minutes.
TOP-004-2	R5.	Each Transmission Operator shall make every effort to remain connected to the Interconnection. If the Transmission Operator determines that by remaining interconnected, it is in imminent danger of violating an IROL or SOL, the Transmission Operator may take such actions, as it deems necessary, to protect its area.	N/A	N/A	N/A	The Transmission Operator did not make every effort to remain connected to the Interconnection except when the Transmission Operator determined that by remaining

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						interconnected, it was in imminent danger of violating an IROL or SOL.
TOP-004-2	R6.	Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including:	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include information required by one of the subrequirements R6.1 thru R6.4	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include information required by 2 of the subrequirements R6.1 thru R6.4.	The Transmission Operator, individually and jointly with other Transmission Operators, developed, maintained, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability, but failed to include information required by 3 of the subrequirements R6.1 thru R6.4.	The Transmission Operator, failed to develop, maintain, and implemented formal policies and procedures to provide for transmission reliability, addressing the execution and coordination of activities that impact inter- and intra-Regional reliability. If formal policies and procedures were developed, such policies and procedures failed to include any of the information required in subrequirements R6.1 thru R6.4.
TOP-004-2	R6.1.	Monitoring and controlling voltage levels and real and reactive power flows.	N/A	N/A	N/A	N/A
TOP-004-2	R6.2.	Switching transmission elements.	N/A	N/A	N/A	N/A
TOP-004-2	R6.3.	Planned outages of transmission elements.	N/A	N/A	N/A	N/A
TOP-004-2	R6.4.	Responding to IROL and SOL violations.	N/A	N/A	N/A	N/A
TOP-007-0	R1.	A Transmission Operator shall inform its Reliability Coordinator when an IROL or SOL has been exceeded and the actions being taken to return the system to within	N/A	N/A	The Transmission Operator informed its Reliability Coordinator when an IROL or SOL had been exceeded but	The Transmission Operator failed to inform its Reliability Coordinator when an IROL or SOL had

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		limits.			failed to provide the actions being taken to return the system to within limits.	been exceeded.
TOP-007-0	R2.	Following a Contingency or other event that results in an IROL violation, the Transmission Operator shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes.	Following a Contingency or other event that resulted in an IROL violation of a magnitude of 5% or less, the Transmission Operator failed to return its transmission system to within the IROL in less than or equal to 35 minutes.	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within the IROL in accordance with the following: (a) an IROL with a magnitude of 5% or less for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (b) an IROL with a magnitude of more than 5% up to (and including) 10% for a period of time less than or equal to 40 minutes, or (c) an IROL with a magnitude of more than 10% up to (and including) 15% for a period of time less than or equal to 35 minutes.	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within the IROL in accordance with the following: (a) an IROL with a magnitude of 5% or less for a period of time greater than 45 minutes, or (b) an IROL with a magnitude of more than 5% up to (and including) 10% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude of more than 10% up to (and including) 15% for a period of time greater than 35 minutes but less than or equal to 45 minutes, or (d) an IROL with a magnitude of more than 15% up to (and including) 20% for a	Following a Contingency or other event that resulted in an IROL violation, the Transmission Operator failed to return its transmission system to within the IROL in accordance with the following: (a) an IROL with a magnitude of more than 10% up to (and including) 15% for a period of time greater than 45 minutes, or (b) an IROL with a magnitude of more than 15% up to (and including) 20% for a period of time greater than 40 minutes, or (c) an IROL with a magnitude of more than 20% up to (and including) 25% for a period of time greater than 35 minutes, or (d) an IROL with a magnitude of more than 25% for a period of greater than 30 minutes.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					period of time less than or equal to 40 minutes, or (e) an IROL with a magnitude of more than 20% up to (and including) 25% for a period of time less than or equal to 35 minutes.	
TOP-007-0	R3.	A Transmission Operator shall take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to comply with Requirement R 2.	N/A	N/A	N/A	The Transmission Operator failed to take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to return the transmission system to IROL within 30 minutes.
TOP-007-0	R4.	The Reliability Coordinator shall evaluate actions taken to address an IROL or SOL violation and, if the actions taken are not appropriate or sufficient, direct actions required to return the system to within limits.	N/A	N/A	N/A	The Reliability Coordinator failed to evaluate actions taken to address an IROL or SOL violation and, if the actions taken were not appropriate or sufficient, direct actions required to return the system to within limits.
TOP-008-1	R1.	The Transmission Operator experiencing or contributing to an IROL or SOL violation shall take immediate steps to relieve the condition, which may include shedding firm load.	N/A	N/A	N/A	The Transmission Operator experiencing or contributing to an IROL or SOL violation failed to take immediate steps to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						relieve the condition, which may have included shedding firm load.
TOP-008-1	R2.	Each Transmission Operator shall operate to prevent the likelihood that a disturbance, action, or inaction will result in an IROL or SOL violation in its area or another area of the Interconnection. In instances where there is a difference in derived operating limits, the Transmission Operator shall always operate the Bulk Electric System to the most limiting parameter.	N/A	N/A	The Transmission Operator operated to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection but failed to operate the Bulk Electric System to the most limiting parameter in instances where there was a difference in derived operating limits.	The Transmission Operator failed to operate to prevent the likelihood that a disturbance, action, or inaction would result in an IROL or SOL violation in its area or another area of the Interconnection.
TOP-008-1	R3.	The Transmission Operator shall disconnect the affected facility if the overload on a transmission facility or abnormal voltage or reactive condition persists and equipment is endangered. In doing so, the Transmission Operator shall notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection prior to switching, if time permits, otherwise, immediately thereafter.	N/A	N/A	The Transmission Operator disconnected the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered but failed to notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection either prior to	The Transmission Operator failed to disconnect the affected facility when the overload on a transmission facility or abnormal voltage or reactive condition persisted and equipment was endangered.

Complete Violation Severity Level Matrix (TOP)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					switching, if time permitted, otherwise, immediately thereafter.	
TOP-008-1	R4.	The Transmission Operator shall have sufficient information and analysis tools to determine the cause(s) of SOL violations. This analysis shall be conducted in all operating timeframes. The Transmission Operator shall use the results of these analyses to immediately mitigate the SOL violation.	N/A	N/A	The Transmission Operator had sufficient information and analysis tools to determine the cause(s) of SOL violations and used the results of these analyses to immediately mitigate the SOL violation(s), but failed to conduct these analyses in all operating timeframes.	The Transmission Operator failed to have sufficient information and analysis tools to determine the cause(s) of SOL violations or failed to use the results of analyses to immediately mitigate the SOL violation.

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-001-0.1	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I. To be considered valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-001-0.1	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-001-0.1	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-001-0.1	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category A of Table 1 (no contingencies). The specific elements selected (from each of the following categories) shall be acceptable to the associated Regional Reliability	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Organization(s).				
TPL-001-0.1	R1.3.1.	Cover critical system conditions and study years as deemed appropriate by the entity performing the study.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-001-0.1	R1.3.2.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system testing) AND most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.
TPL-001-0.1	R1.3.3.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system simulation testing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						show marginal conditions that may require longer lead-time solutions.
TPL-001-0.1	R1.3.4.	Have established normal (pre-contingency) operating procedures in place.	N/A	N/A	N/A	No precontingency operating procedures are in place for existing facilities.
TPL-001-0.1	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-001-0.1	R1.3.6.	Be performed for selected demand levels over the range of forecast system demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-001-0.1	R1.3.7.	Demonstrate that system performance meets Table 1 for Category A (no contingencies).	N/A	N/A	N/A	No past or current study results exist showing pre-contingency system analysis.
TPL-001-0.1	R1.3.8.	Include existing and planned facilities.	The responsible entity’s transmission model used for past or current studies and/or	The responsible entity’s transmission model used for past or current studies and/or	N/A	The responsible entity's transmission model used for past or current studies and/or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.		system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-001-0.1	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-001-0.1	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category A.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category A planning requirements.
TPL-001-0.1	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-001-0_R1, the Planning Authority and Transmission Planner shall each:	N/A	The responsible entity has failed to review the continuing need for previously identified facility additions through subsequent annual assessments. (R2.2)	The responsible entity provided documented evidence of corrective action plans in order to satisfy Category A planning requirements, but failed to include an implementation schedule with in-service dates (R2.1.1 and R2.1.2) OR The responsible entity	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category A planning requirements. (R2.1)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					failed to consider necessary lead times to implement its corrective action plan. (R2.1.3)	
TPL-001-0.1	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	N/A
TPL-001-0.1	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	N/A	N/A	N/A	N/A
TPL-001-0.1	R3.	The Planning Authority and Transmission Planner shall each document the results of these reliability assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization
TPL-002-0b	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:	25% or less of the sub-components.	more than 25% but less than 50% of the sub-components.	50% or more but less than 75% of the sub-components.	75% or more of the sub-components.
TPL-002-0b	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-002-0b	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-002-0b	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-002-0b	R1.3.1.	Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies	N/A	The responsible entity provided evidence through current or past studies and/or	N/A	The responsible entity did not provided evidence through current or past studies

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.		system simulation testing that selected NERC Category B contingencies were evaluated, however, no rational was provided to indicate why the remaining Category B contingencies for their system were not evaluated.		and/or system simulation testing to indicate that any NERC Category B contingencies were evaluated.
TPL-002-0b	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-002-0b	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies (and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are no longer valid.
TPL-002-0b	R1.3.4.	Be conducted beyond the five-year horizon	N/A	N/A	N/A	The responsible entity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		only as needed to address identified marginal conditions that may have longer lead-time solutions.				failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system simulation testing show marginal conditions that may require longer lead-time solutions.
TPL-002-0b	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-002-0b	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast system Demands.	N/A	N/A	N/A	The responsible entity has failed to produce evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-002-0b	R1.3.7.	Demonstrate that system performance meets Category B contingencies.	N/A	N/A	N/A	No past or current study results exist showing Category B

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						contingency system analysis.
TPL-002-0b	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-002-0b	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-002-0b	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-002-0b	R1.3.11.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect	The responsible entity's transmission model used for past or current studies is deficient with respect

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					to the effects of planned control devices.	to the effects of existing control devices.
TPL-002-0b	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-002-0b	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category B of Table I.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category B planning requirements.
TPL-002-0b	R1.5.	Consider all contingencies applicable to Category B.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to 25% or less of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	The responsible entity has considered the NERC Category B contingencies applicable to their system, but was deficient 75% or more of all applicable contingencies.
TPL-002-0b	R2.	When System simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-002-0_R1, the Planning Authority and Transmission Planner shall each:	N/A	The responsible entity has failed to review the continuing need for previously identified facility	The responsible entity provided documented evidence of corrective action plans in order to satisfy Category B	The responsible entity has failed to provide documented evidence of corrective action plans in order to

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				additions through subsequent annual assessments. (R2.2)	planning requirements, but failed to include a implementation schedule with in-service dates (R2.1.1 and R2.1.2) OR The responsible entity failed to consider necessary lead times to implement its corrective action plan. (R2.1.3)	satisfy Category B planning requirements. (R2.1)
TPL-002-0b	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	N/A
TPL-002-0b	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	N/A
TPL-002-0b	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	N/A
TPL-002-0b	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	N/A
TPL-002-0b	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.	N/A	N/A	N/A	N/A
TPL-002-0b	R3.	The Planning Authority and Transmission Planner shall each document the results of its Reliability Assessments and corrective plans and shall annually provide the results to its respective Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Regional Reliability Organization(s) as required by the Regional Reliability Organization.		respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.
TPL-003-0a	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:	The responsible entity is non-compliant with 25% or less of the sub-components.	The responsible entity is non-compliant with more than 25% but less than 50% of the sub-components.	The responsible entity is non-compliant with 50% or more but less than 75% of the sub-components.	The responsible entity is non-compliant with 75% or more of the sub-components.
TPL-003-0a	R1.1.	Be made annually.	N/A	N/A	N/A	The assessments were not made on an annual basis.
TPL-003-0a	R1.2.	Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.	The responsible entity has failed to demonstrate a valid assessment for the long-term period, but a valid assessment for the near-term period exists.	The responsible entity has failed to demonstrate a valid assessment for the near-term period, but a valid assessment for the long-term period exists.	N/A	The responsible entity has failed to demonstrate a valid assessment for the near-term period AND long-term planning period.
TPL-003-0a	R1.3.	Be supported by a current or past study and/or system simulation testing that	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with	The responsible entity is non-compliant with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	25% or less of the sub-components.	more than 25% but less than 50% of the sub-components.	50% or more but less than 75% of the sub-components.	75% or more of the sub-components.
TPL-003-0a	R1.3.1.	Be performed and evaluated only for those Category C contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.	N/A	The responsible entity provided evidence through current or past studies that selected NERC Category C contingencies were evaluated, however, no rational was provided to indicate why the remaining Category C contingencies for their system were not evaluated.	N/A	The responsible entity did not provided evidence through current or past studies to indicate that any NERC Category C contingencies were evaluated.
TPL-003-0a	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	The responsible entity has failed to cover critical system conditions and study years as deemed appropriate.
TPL-003-0a	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	The responsible entity's most recent long-term studies (and/or system simulation testing) were not performed in the most recent annual	The responsible entity's most recent near-term studies (and/or system simulation testing) were not performed in the most recent	N/A	The responsible entity's most recent near-term studies (and/or system simulation testing) AND most recent long-term studies

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.	annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system testing) are no longer valid.		(and/or system testing) were not performed in the most recent annual period AND significant system changes (actual or proposed) indicate that past studies (and/or system simulation testing) are no longer valid.
TPL-003-0a	R1.3.4.	Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.	N/A	N/A	N/A	The responsible entity failed to produce evidence of a past or current year long-term study and/or system simulation testing (beyond 5-year planning horizon) when past or current year near-term studies and/or system testing show marginal conditions that may require longer lead-time solutions.
TPL-003-0a	R1.3.5.	Have all projected firm transfers modeled.	The system model(s) used for current or past analysis did not properly represent up to (but less than) 25% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 25% or more but less than 50% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 50% or more but less than 75% of the firm transfers to/from the responsible entity's service territory.	The system model(s) used for current or past analysis did not properly represent 75% or more of the firm transfers to/from the responsible entity's service territory.
TPL-003-0a	R1.3.6.	Be performed and evaluated for selected demand levels over the range of forecast	N/A	N/A	N/A	The responsible entity has failed to produce

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		system demands.				evidence of a valid current or past study and/or system simulation testing reflecting analysis over a range of forecast system demands.
TPL-003-0a	R1.3.7.	Demonstrate that System performance meets Table 1 for Category C contingencies.	N/A	N/A	N/A	No past or current study results exists showing Category C contingency system analysis.
TPL-003-0a	R1.3.8.	Include existing and planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects existing facilities, but is deficient in reflecting planned facilities.	The responsible entity's transmission model used for past or current studies and/or system simulation testing properly reflects planned facilities, but is deficient in reflecting existing facilities.	N/A	The responsible entity's transmission model used for past or current studies and/or system simulation testing is deficient in reflecting existing AND planned facilities.
TPL-003-0a	R1.3.9.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet System performance.	N/A	N/A	N/A	The responsible entity has failed to ensure in a past or current study and/or system simulation testing that sufficient reactive power resources are available to meet required system performance.
TPL-003-0a	R1.3.10.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	The responsible entity's transmission model used for past or current studies is	The responsible entity's transmission model used for past or current studies is

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficient with respect to the effects of planned protection systems, including any backup or redundant systems.	deficient with respect to the effects of existing protection systems, including any backup or redundant systems.
TPL-003-0a	R1.3.11.	Include the effects of existing and planned control devices.	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of planned control devices.	The responsible entity's transmission model used for past or current studies is deficient with respect to the effects of existing control devices.
TPL-003-0a	R1.3.12.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those Demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	The responsible entity's transmission model used for past or current studies is deficient with respect to the inclusion of planned maintenance outages of bulk electric transmission facilities.
TPL-003-0a	R1.4.	Address any planned upgrades needed to meet the performance requirements of Category C.	N/A	N/A	N/A	The responsible entity has failed to demonstrate that a corrective action plan exists in order to satisfy Category C planning requirements.
TPL-003-0a	R1.5.	Consider all contingencies applicable to Category C.	The responsible entity has considered the NERC Category C contingencies applicable to their	The responsible entity has considered the NERC Category C contingencies applicable to their	The responsible entity has considered the NERC Category C contingencies applicable to their	The responsible entity has considered the NERC Category C contingencies applicable to their

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			system, but was deficient with respect to 25% or less of all applicable contingencies.	system, but was deficient with respect to more than 25% but less than 50% of all applicable contingencies.	system, but was deficient with respect to more than 50% but less than 75% of all applicable contingencies.	system, but was deficient 75% or more of all applicable contingencies.
TPL-003-0a	R2.	When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-003-0_R1, the Planning Authority and Transmission Planner shall each:	N/A	The responsible entity has failed to review the continuing need for previously identified facility additions through subsequent annual assessments. (R2.2)	The responsible entity provided documented evidence of corrective action plans in order to satisfy Category C planning requirements, but failed to include an implementation schedule with in-service dates. (R2.1.1 and R2.1.2) OR The responsible entity failed to consider necessary lead times to implement its corrective action plan. (R2.1.3)	The responsible entity has failed to provide documented evidence of corrective action plans in order to satisfy Category C planning requirements. (R2.1)
TPL-003-0a	R2.1.	Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:	N/A	N/A	N/A	N/A
TPL-003-0a	R2.1.1.	Including a schedule for implementation.	N/A	N/A	N/A	N/A
TPL-003-0a	R2.1.2.	Including a discussion of expected required in-service dates of facilities.	N/A	N/A	N/A	N/A
TPL-003-0a	R2.1.3.	Consider lead times necessary to implement plans.	N/A	N/A	N/A	N/A
TPL-003-0a	R2.2.	Review, in subsequent annual assessments, (where sufficient lead time exists), the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		continuing need for identified system facilities. Detailed implementation plans are not needed.				
TPL-003-0a	R3.	The Planning Authority and Transmission Planner shall each document the results of these Reliability Assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments and corrective plans but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.	N/A	The responsible entity DID NOT document the results of its annual reliability assessments and corrective plans AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.
TPL-004-0	R1.	The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Table I. To be valid, the Planning Authority's and Transmission Planner's assessment shall:	The responsible entity is non-compliant with one of the sub-components of requirement R1.3 (R1.3.1 through R1.3.9). OR The responsible entity has considered the NERC Category D contingencies applicable to their system, but was deficient with respect to 5% or less of all applicable contingencies. (R1.4)	The responsible entity is non-compliant with two of the sub-components of requirement R1.3 (R1.3.1 through 1.3.9). OR The responsible entity has considered the NERC Category D contingencies applicable to their system, but was deficient with respect to more than 5% up to (and including) 10% of all applicable contingencies. (R1.4)	The responsible entity is non-compliant with three of the sub-components of requirement R1.3 (R1.3.1 through 1.3.9). OR The responsible entity has considered the NERC Category D contingencies applicable to their system, but was deficient with respect to more than 10% up to (and including) 15% of all applicable contingencies. (R1.4)	The responsible entity did not perform the transmission assessments annually. (R1.1) OR The responsible entity has failed to demonstrate a valid assessment for the near-term planning period. (R1.2) OR The responsible entity is non-compliant with four or more of the sub-components of requirement R1.3 (R1.3.1 through 1.3.9).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The responsible entity has considered the NERC Category D contingencies applicable to its system, but was deficient with respect to more than 15% of all applicable contingencies. (R1.4)
TPL-004-0	R1.1.	Be made annually.	N/A	N/A	N/A	N/A
TPL-004-0	R1.2.	Be conducted for near-term (years one through five).	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.	Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category D contingencies of Table I. The specific elements selected (from within each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.1.	Be performed and evaluated only for those Category D contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.2.	Cover critical system conditions and study years as deemed appropriate by the responsible entity.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (TPL)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
TPL-004-0	R1.3.3.	Be conducted annually unless changes to system conditions do not warrant such analyses.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.4.	Have all projected firm transfers modeled.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.5.	Include existing and planned facilities.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.6.	Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.7.	Include the effects of existing and planned protection systems, including any backup or redundant systems.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.8.	Include the effects of existing and planned control devices.	N/A	N/A	N/A	N/A
TPL-004-0	R1.3.9.	Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.	N/A	N/A	N/A	N/A
TPL-004-0	R1.4.	Consider all contingencies applicable to Category D.	N/A	N/A	N/A	N/A
TPL-004-0	R2.	The Planning Authority and Transmission Planner shall each document the results of its reliability assessments and shall annually provide the results to its entities' respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.	N/A	The responsible entity documented the results of its reliability assessments but did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.	N/A	The responsible entity DID NOT document the results of its annual reliability assessments AND did not annually provide them to its respective NERC Regional Reliability Organization(s) as required by the Regional Reliability Organization.

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-001-2	R1.	Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 5% or less of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting between 5-10% of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting 10-15%, inclusive, of their individual and neighboring areas voltage levels and Mvar flows.	The applicable entity did not ensure the development and/or maintenance and/or implementation of formal policies and procedures, as directed by the requirement, affecting greater than 15% of their individual and neighboring areas voltage levels and Mvar flows.
VAR-001-2	R2.	Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 95% but less than 100% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 90% but less than 95% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired 85% but less than 90% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.	The Transmission Operator acquired less than 85% of the reactive resources within its area needed to protect the voltage levels under normal and Contingency conditions including the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.
VAR-001-2	R3.	The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.	N/A	N/A	N/A	The Transmission Operator did not specify criteria that exempts generators from compliance with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the requirements defined in Requirement 4, and Requirement 6.1. to all of the parties involved.
VAR-001-2	R3.1.	Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing one or more entities. The missing entities shall represent less than 25% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing two or more entities. The missing entities shall represent less than 50% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing three or more entities. The missing entities shall represent less than 75% of those eligible for the list	The Transmission Operator maintain the list of generators in its area that are exempt from following a voltage or Reactive Power schedule but is missing four or more entities. The missing entities shall represent 75% or more of those eligible for the list.
VAR-001-2	R3.2.	For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.	The Transmission Operator failed to notify up to 25% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 25% up to 50% of the associated Generator Owners of each generator that are on this exemption list.	The Transmission Operator failed to notify 50% up to 75% of the associated Generator Owner of each generator that are on this exemption list.	The Transmission Operator failed to notify 75% up to 100% of the associated Generator Owner of each generator that are on this exemption list.
VAR-001-2	R4.	Each Transmission Operator shall specify a voltage or Reactive Power schedule [4] at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the	N/A	N/A	The Transmission Operator provide Voltage or Reactive Power schedules were for some but not all generating units as required in R4.	The Transmission Operator provide No evidence that voltage or Reactive Power schedules were provided to Generator Operators as required

[4] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).				in R4.
VAR-001-2	R5. (Retired)	Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 5% or less of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting between 5-10% of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting 10-15%, inclusive, of its reactive requirements.	The applicable entity did not arrange for reactive resources, as directed by the requirement, affecting greater than 15% of its reactive requirements.
VAR-001-2	R6.	The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting 5% or less of the required resources.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting between 5-10% of the required resources.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting 10-15%, inclusive, of the required resources.	The applicable entity did not know the status of all transmission reactive power resources, including the status of voltage regulators and power system stabilizers, as directed by the requirement, affecting 15% or greater of required resources.
VAR-001-2	R6.1.	When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.	N/A	N/A	N/A	The Transmission Operator has not provided evidence to show that directives were issued to the Generator Operator to maintain or change either its voltage schedule or its Reactive Power

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						schedule in accordance with R6.1.
VAR-001-2	R7.	The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 5% or less of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting between 5-10% of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting 10-15%, inclusive, of the required devices.	The applicable entity was not able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow, affecting greater than 15% of the required devices.
VAR-001-2	R8.	Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 5% or less of the required resources.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting between 5-10% of the required resources.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting 10-15%, inclusive, of the required resources.	The applicable entity did operate or direct the operation of capacitive and inductive reactive resources or load shedding within its area, as directed by the requirement, affecting greater than 15% of the required resources.
VAR-001-2	R9.	Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to support its voltage under first Contingency conditions.	The Transmission Operator maintains 95% or more of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 85% or more but less than 95% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains 75% or more but less then 85% of the reactive resources needed to support its voltage under first Contingency conditions.	The Transmission Operator maintains less than 75% of the reactive resources needed to support its voltage under first Contingency conditions.
VAR-001-2	R9.1.	Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.	The applicable entity did not disperse and/or locate the reactive resources, as directed in	The applicable entity did not disperse and/or locate the reactive resources, as	The applicable entity did not disperse and/or locate the reactive resources, as directed	The applicable entity did not disperse and/or locate the reactive resources, as directed

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the requirement, affecting 5% or less of the resources.	directed in the requirement, affecting between 5-10% of the resources.	in the requirement, affecting 10-15%, inclusive, of the resources.	in the requirement, affecting greater than 15% of the resources.
VAR-001-2	R10.	Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 5% or less of the violations.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting between 5-10% of the violations.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting 10-15%, inclusive, of the violations.	The applicable entity did not correct the IROL or SOL violations and/or complete the required IROL or SOL violation reporting, as directed by the requirement, affecting greater than 15% of the violations.
VAR-001-2	R11.	After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes and a timeframe for making these changes, but failed to provide technical justification for these changes.	The Transmission Operator provided documentation to the Generator Owner specifying required step-up transformer tap changes, but failed to provide a timeframe for making these changes and technical justification for these changes.	The Transmission Operator failed to provide documentation to the Generator Owner specifying required step-up transformer tap changes, a timeframe for making these changes, and technical justification for these changes.	N/A
VAR-001-2	R12.	The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.	N/A	N/A	N/A	The Transmission Operator has failed to direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1b	R1.	The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator.	N/A	N/A	N/A	The responsible entity did not operate each generator in the automatic voltage control mode and failed to notify the Transmission Operator as identified in R1.
VAR-002-1.1b	R2.	Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings. [1] as directed by the Transmission Operator	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by 5% or less.	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by more than 5% up to (and including) 10% OR When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by more than 10% up to (and including) 15%	When directed by the Transmission Operator to maintain the generator voltage or reactive power output the Generator Operator failed to meet the directed values by more than 15%. OR When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Reactive Power schedule directed by the Transmission Operator. OR The Generator Operator failed to provide an explanation of why the voltage schedule could not be met.		directed by the Transmission Operator and the Generator Operator failed to provide an explanation of why the voltage schedule could not be met.
VAR-002-1.1b	R2.1.	When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R2.2.	When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R3.	Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:	N/A	N/A	The Generator Operator failed to notify the Transmission Operator within 30 minutes of the information as specified in either R3.1 or R3.2	The Generator Operator failed to notify the Transmission Operator within 30 minutes of the information as specified in both R3.1 and R3.2
VAR-002-1.1b	R3.1.	A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1b	R3.2.	A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.	The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner one of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 30, but less than or equal to 35 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner two of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 35, but less than or equal to 40 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner three of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 40, but less than or equal to 45 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner any of the types of data as specified in R4.1.1 and R 4.1.2 and 4.1.3 and 4.1.4 OR The information was provided in more than 45 calendar days of the request.
VAR-002-1.1b	R4.1.	For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.1.	Tap settings.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.2.	Available fixed tap ranges.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.3.	Impedance data.	N/A	N/A	N/A	N/A
VAR-002-1.1b	R4.1.4.	The +/- voltage range with step-change in % for load-tap changing transformers.	N/A	N/A	N/A	N/A

Complete Violation Severity Level Matrix (VAR)
Encompassing All Commission-Approved Reliability Standards

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
VAR-002-1.1b	R5.	After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.	N/A	N/A	N/A	The responsible entity failed to ensure that transformer tap positions were changed according to the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.
VAR-002-1.1b	R5.1.	If the Generator Operator can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.	N/A	N/A	N/A	The responsible entity failed to notify the Transmission Operator and to provide technical justification.
VAR-002-WECC-1	R1.	Generator Operators and Transmission Operators shall have AVR in service and in automatic voltage control mode 98% of all operating hours for synchronous generators or synchronous condensers. Generator Operators and Transmission Operators may exclude hours for R1.1 through R1.10 to achieve the 98% requirement. [*See Standard pdf for R1.1 through R1.10*]	AVR is in service less than 98% but at least 90% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.	AVR is in service less than 90% but at least 80% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.	AVR is in service less than 80% but at least 70% or more of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.	AVR is in service less than 70% of all hours during which the synchronous generating unit or synchronous condenser is on line for each calendar quarter.
VAR-002-WECC-1	R2.	Generator Operators and Transmission Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.10.	There shall be a Lower Level of non-compliance if documentation is incomplete with any requirement R1.1	There shall be a Moderate Level of non-compliance if the Generator Operator does not have documentation to	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			through R1.10.	demonstrate compliance with any requirement R1.1 through R1.10.		
VAR-501-WECC-1	R1.	Generator Operators shall have PSS in service 98% of all operating hours for synchronous generators equipped with PSS. Generator Operators may exclude hours for R1.1 through R1.12 to achieve the 98% requirement. [*See Standard pdf for R1.1 through R1.12*]	PSS is in service less than 98% but at least 90% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.	PSS is in service less than 90% but at least 80% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.	PSS is in service less than 80% but at least 70% or more of all hours during which the synchronous generating unit is on line for each calendar quarter.	PSS is in service less than 70% of all hours during which the synchronous generating unit is on line for each calendar quarter.
VAR-501-WECC-1	R2.	Generator Operators shall have documentation identifying the number of hours excluded for each requirement in R1.1 through R1.12.	There shall be a Lower Level of non-compliance if documentation is incomplete with any requirement R1.1 through R1.12.	There shall be a Moderate Level of non-compliance if the Generator Operator does not have documentation to demonstrate compliance with any requirement R1.1 through R1.12.	N/A	N/A

NERC Reliability Standards VSL Change History Table:

Date	Standard	Requirement	Action
9/25/12	BAL-005-0.2b, EOP-001-0.1b, EOP-002-3.1, PER-001-0.2 & TOP-002-2.1b		FERC approved Errata - Added
TBD	BAL-005-0.2b, CIP-001-2a, CIP-003-3, CIP-003-4, CIP-005-3a, CIP-005-4a, CIP-007-3, CIP-007-4, EOP-004-1, FAC-002-1, FAC-008-1, FAC-008-3, FAC-010-2.1, FAC-011-2, FAC-013-2, INT-007-1, IRO-016-1, NUC-001-2, PRC-010-0, PRC-022-1, VAR-001-2		Various VSLs retired as part of the Paragraph 81 project (Project 2013-02)

Standard Version	Requirement Name	Requirement Text
BAL-005-0.2b	R2.	Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard.
CIP-003-3	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-3	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
CIP-003-3	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
CIP-003-3	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
CIP-003-3	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
CIP-003-3	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-4	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
CIP-003-4	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
CIP-003-4	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-005-3a	R2.6.	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

Standard Version	Requirement Name	Requirement Text
CIP-005-4a	R2.6.	Appropriate Use Banner —Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
CIP-007-3	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
EOP-005-2	R3.1.	If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary.
FAC-002-1	R2.	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).
FAC-008-1	R2.	The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request.
FAC-008-1	R3.	If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why.
FAC-008-3	R4.	Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request.

Standard Version	Requirement Name	Requirement Text
FAC-008-3	R5.	If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why.
FAC-010-2.1	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.
FAC-011-2	R5.	If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why.
FAC-013-2	R3.	If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why.
INT-007-1	R1.2.	All reliability entities involved in the Arranged Interchange are currently in the NERC registry.
IRO-016-1	R2.	The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both.
NUC-001-2	R9.1.	Administrative elements:
NUC-001-2	R9.1.1.	Definitions of key terms used in the agreement.
NUC-001-2	R9.1.2.	Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.
NUC-001-2	R9.1.3.	A requirement to review the agreement(s) at least every three years.
NUC-001-2	R9.1.4.	A dispute resolution mechanism.

Standard Version	Requirement Name	Requirement Text
PRC-010-0	R2.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).
PRC-022-1	R2.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.
VAR-001-2	R5.	Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider.

A. Introduction

1. **Title:** **Automatic Generation Control**

2. **Number:** BAL-005-0.2b

3. **Purpose:** This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.

4. **Applicability:**

   4.1. Balancing Authorities

   4.2. Generator Operators

   4.3. Transmission Operators

   4.4. Load Serving Entities

5. **Effective Date:** May 13, 2009

B. Requirements

R1. All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.

R1.1. Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.

R1.2. Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.

R1.3. Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.

R2. Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retired)

R3. A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.

R4. A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.

R5. A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.

R6. The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control. If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

R7. The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.

R8. The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.

R8.1. Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary source. This overall installation shall provide a minimum availability of 99.95%.

R9. The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.

R9.1. Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.

R10. The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.

R11. Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.

R12. Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.

R12.1. Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed-upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.

R12.2. Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.

R12.3. Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.

R13. Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.

R14. The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance. As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area.

R15. The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical

locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

R16. The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

1.1.1. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.

1.1.2. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

1.3.1. Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.

1.3.2. Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as the ACE charts and/or samples used to calculate Balancing Authority or

Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Effective Date: August 27, 2008 (U.S.)

Interpretation of BAL-005-0 Automatic Generation Control, R17

Request for Clarification received from PGE on July 31, 2007

PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

BAL-005-0

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25% of full scale
Remote terminal unit	≤ 0.25% of full scale
Potential transformer	≤ 0.30% of full scale
Current transformer	≤ 0.50% of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to "annually check and calibrate" does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to "annually check and calibrate" the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system

operator. Frequency inputs from other sources that are for reference only are excluded. The time error and frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-3

3. Purpose: Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-003-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-3 Requirement R2.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

3	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets. (Retired)

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s). (Retired)

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s). (Retired)

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. (Retired)

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented. (Retired)

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information. (Retired)

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2. (R1.2 retired)

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3. (Retired)

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				within thirty calendar days of the effective date.	
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3. (Retired)	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).
R3.1. (Retired)	LOWER	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).
R3.2. (Retired)	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3. (Retired)	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.2. (Retired)	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	The Responsible Entity has established but not documented a change	The Responsible Entity has established but not documented both a change control process and configuration management	The Responsible Entity has not established and documented a change control process OR	The Responsible Entity has not established and documented a change control process AND

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		control process OR The Responsible Entity has established but not documented a configuration management process.	process.	The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a configuration management process.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R1.2, R3, R3.1, R3.2, R3.3, and R4.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-3a

3. Purpose: Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability

4.1. Within the text of Standard CIP-005-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-3, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-3 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity	

		shall “implement and maintain” a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3a	02/16/10	Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010	Interpretation
3a	02/02/11	Approved by FERC	
3a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal

Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. (Retired)

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4;

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	and Standard CIP-009-4.	and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter.		
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6. (Retired)	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.			
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to designated response personnel.	Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	Revised.
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"
4a	4/19/12	FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3a, 4a	TBD	R2.6 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-3

3. Purpose: Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. Applicability:

4.1. Within the text of Standard CIP-007-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-3 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical)	

		Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
3	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures. (Retired)

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, **but did not document** that testing is performed as required in R1.2. OR The Responsible Entity did not document the test results as required in R1.3.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).

		testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).		
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.
R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program **but** did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.

R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.

R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
R5.1.1.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

			manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).		
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.
R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 **but** did not maintain records as specified in R7.3. (Retired)	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A
R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3. (Retired)	LOWER	N/A	N/A	N/A	N/A

R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A
R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
3, 4	TBD	R7.3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Restoration from Blackstart Resources**

2. Number: EOP-005-2

3. Purpose: Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

4. Applicability:

4.1. Transmission Operators.

4.2. Generator Operators.

4.3. Transmission Owners identified in the Transmission Operators restoration plan.

4.4. Distribution Providers identified in the Transmission Operators restoration plan.

5. Proposed Effective Date: Twenty-four months after the first day of the first calendar quarter following applicable regulatory approval. In those jurisdictions where no regulatory approval is required, all requirements go into effect twenty-four months after Board of Trustees adoption.

B. Requirements

R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include: *[Time Horizon = Operations Planning]*

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

R1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

R1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.

R2. Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan. *[Time Horizon = Operations Planning]*

R3. Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule. *[Time Horizon = Operations Planning]*

R3.1. If there are no changes to the previously submitted restoration plan, the Transmission Operator shall confirm annually on a predetermined schedule to its Reliability Coordinator that it has reviewed its restoration plan and no changes were necessary. (Retired)

R4. Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan. *[Time Horizon = Operations Planning]*

R4.1. Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.

R5. Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date. *[Time Horizon = Operations Planning]*

R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify: *[Time Horizon = Long-term Planning]*

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

R7. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each

affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration. *[Time Horizon = Real-time Operations]*

R8. Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator. *[Time Horizon = Real-time Operations]*

R9. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include: *[Time Horizon = Operations Planning]*

R9.1. The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

R9.2. A list of required tests including:

R9.2.1. The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.

R9.2.2. The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

R9.3. The minimum duration of each of the required tests.

R10. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following: *[Time Horizon = Operations Planning]*

R10.1. System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.

R10.2. Restoration priorities.

R10.3. Building of cranking paths.

R10.4. Synchronizing (re-energized sections of the System).

R11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks. *[Time Horizon = Operations Planning]*

R12. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator. *[Time Horizon = Operations Planning]*

R13. Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. *[Time Horizon = Operations Planning]*

R14. Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. *[Time Horizon = Operations Planning]*

R15. Each Generator Operator with a Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator's restoration plan within 24 hours following such change. *[Time Horizon = Operations Planning]*

R16. Each Generator Operator with a Blackstart Resource shall perform Blackstart Resource tests, and maintain records of such testing, in accordance with the testing requirements set by the Transmission Operator to verify that the Blackstart Resource can perform as specified in the restoration plan. *[Time Horizon = Operations Planning]*

R16.1. Testing records shall include at a minimum: name of the Blackstart Resource, unit tested, date of the test, duration of the test, time required to start the unit, an indication of any testing requirements not met under Requirement R9.

R16.2. Each Generator Operator shall provide the blackstart test results within 30 calendar days following a request from its Reliability Coordinator or Transmission Operator.

R17. Each Generator Operator with a Blackstart Resource shall provide a minimum of two hours of training every two calendar years to each of its operating personnel responsible for the startup of its Blackstart Resource generation units and energizing a bus. The training program shall include training on the following: *[Time Horizon = Operations Planning]*

R17.1. System restoration plan including coordination with the Transmission Operator.

R17.2. The procedures documented in Requirement R14.

R18. Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator. *[Time Horizon = Operations Planning]*

C. Measures

M1. Each Transmission Operator shall have a dated, documented System restoration plan developed in accordance with Requirement R1 that has been approved by its Reliability Coordinator as shown with the documented approval from its Reliability Coordinator.

M2. Each Transmission Operator shall have evidence such as e-mails with receipts or registered mail receipts that it provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan in accordance with Requirement R2.

M3. Each Transmission Operator shall have documentation such as a dated review signature sheet, revision histories, e-mails with receipts, or registered mail receipts, that it has annually reviewed and submitted the Transmission Operator's restoration plan to its Reliability Coordinator in accordance with Requirement R3.

M4. Each Transmission Operator shall have documentation such as dated review signature sheets, revision histories, e-mails with receipts, or registered mail receipts, that it has updated its restoration plan and submitted it to its Reliability Coordinator in accordance with Requirement R4.

M5. Each Transmission Operator shall have documentation that it has made the latest Reliability Coordinator approved copy of its restoration plan available in its primary and backup control rooms and its System Operators prior to its implementation date in accordance with Requirement R5.

M6. Each Transmission Operator shall have documentation such as power flow outputs, that it has verified that its latest restoration plan will accomplish its intended function in accordance with Requirement R6.

M7. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved shall have evidence such as voice recordings, e-mail, dated computer printouts, or operator logs, that it implemented its restoration plan or restoration plan strategies in accordance with Requirement R7.

M8. If there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service, each Transmission Operator involved in such an event shall have evidence, such as voice recordings, e-mail, dated computer printouts, or operator logs, that it resynchronized shut down areas in accordance with Requirement R8.

M9. Each Transmission Operator shall have documented Blackstart Resource testing requirements in accordance with Requirement R9.

M10. Each Transmission Operator shall have an electronic or hard copy of the training program material provided for its System Operators for System restoration training in accordance with Requirement R10.

M11. Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall have an electronic or hard copy of the training program material provided to their field switching personnel for System restoration training and the corresponding training records including training dates and duration in accordance with Requirement R11.

M12. Each Transmission Operator shall have evidence, such as training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations as requested in accordance with Requirement R12.

M13. Each Transmission Operator and Generator Operator with a Blackstart Resource shall have the dated Blackstart Resource Agreements or mutually agreed upon procedures or protocols in accordance with Requirement R13.

M14. Each Generator Operator with a Blackstart Resource shall have dated documented procedures on file for starting each unit and energizing a bus in accordance with Requirement R14.

M15. Each Generator Operator with a Blackstart Resource shall provide evidence, such as e-mails with receipts or registered mail receipts, showing that it notified its Transmission Operator of any known changes to its Blackstart Resource capabilities within twenty-four hours of such changes in accordance with Requirement R15.

M16. Each Generator Operator with a Blackstart Resource shall maintain dated documentation of its Blackstart Resource test results and shall have evidence such as e-mails with receipts or registered mail receipts, that it provided these records to its Reliability Coordinator and Transmission Operator when requested in accordance with Requirement R16.

M17. Each Generator Operator with a Blackstart Resource shall have an electronic or hard copy of the training program material provided to its operating personnel responsible for the startup and synchronization of its Blackstart Resource generation units and a copy of its dated training records including training dates and durations showing that it has provided training in accordance with Requirement R17.

M18. Each Generator Operator shall have evidence, such as dated training records, that it participated in the Reliability Coordinator's restoration drills, exercises, or simulations if requested to do so in accordance with Requirement R18.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Approved restoration plan and any restoration plans in force since the last compliance audit for Requirement R1, Measure M1.
- Provided the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan for the current calendar year and three prior calendar years for Requirement R2, Measure M2.
- Submission of the Transmission Operator's annually reviewed restoration plan to its Reliability Coordinator for the current calendar year and three prior calendar years for Requirement R3, Measure M3.
- Submission of an updated restoration plan to its Reliability Coordinator for all versions for the current calendar year and the prior three years for Requirement R4, Measure M4.
- The current, restoration plan approved by the Reliability Coordinator and any restoration plans for the last three calendar years that was made available in its control rooms for Requirement R5, Measure M5.
- The verification results for the current, approved restoration plan and the previous approved restoration plan for Requirement R6, Measure M6.
- Implementation of its restoration plan or restoration plan strategies on any occasion for three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R7, Measure M7.
- Resynchronization of shut down areas on any occasion over three calendar years if there has been a Disturbance in which Blackstart Resources have been utilized in restoring the shut down area of the BES to service for Requirement R8, Measure M8.
- The verification process and results for the current Blackstart Resource testing requirements and the last previous Blackstart Resource testing requirements for Requirement R9, Measure M9.
- Actual training program materials or descriptions for three calendar years for Requirement R10, Measure M10.
- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit as well as one previous compliance audit period for Requirement R12, Measure M12.

If a Transmission Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator, applicable Transmission Owner, and applicable Distribution provider shall keep data or evidence to show compliance as identified

below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Actual training program materials or descriptions and actual training records for three calendar years for Requirement R11, Measure M11.

If a Transmission Operator, applicable Transmission owner, or applicable Distribution Provider is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Transmission Operator and Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current Blackstart Resource Agreements and any Blackstart Resource Agreements or mutually agreed upon procedures or protocols in force since its last compliance audit for Requirement R13, Measure M13.

The Generator Operator with a Blackstart Resource shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Current documentation and any documentation in force since its last compliance audit on procedures to start each Blackstart Resources and for energizing a bus for Requirement R14, Measure M14.
- Notification to its Transmission Operator of any known changes to its Blackstart Resource capabilities over the last three calendar years for Requirement R15, Measure M15.
- The verification test results for the current set of requirements and one previous set for its Blackstart Resources for Requirement R16, Measure M16.
- Actual training program materials and actual training records for three calendar years for Requirement R17, Measure M17.

If a Generation Operator with a Blackstart Resource is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Generator Operator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Records of participation in all requested Reliability Coordinator restoration drills, exercises, or simulations since its last compliance audit for Requirement R18, Measure M18.

If a Generation Operator is found non-compliant for any requirement, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	May 2, 2007	Approved by Board of Trustees	Revised
2	TBD	Revisions pursuant to Project 2006-03	Updated testing requirements Incorporated Attachment 1 into the requirements Updated Measures and Compliance to match new Requirements
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	March 17, 2011	Order issued by FERC approving EOP-005-2 (approval effective 5/23/11)	
2	TBD	R3.1 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Coordination of Plans For New Generation, Transmission, and End-User Facilities

2. Number: FAC-002-1

3. Purpose: To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.

4. Applicability:

4.1. Generator Owner

4.2. Transmission Owner

4.3. Distribution Provider

4.4. Load-Serving Entity

4.5. Transmission Planner

4.6. Planning Authority

5. (Proposed) Effective Date: The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:

1.1. Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.

1.2. Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.

1.3. Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.

1.4. Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance under both normal and contingency conditions in accordance with Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0.

1.5. Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected

transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days). (Retired)

C. Measures

M1. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider's documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.

M2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Timeframe

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting

Complaints

1.4. Data Retention

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

1.5. Additional Compliance Information

None

2. Violation Severity Levels (no changes)

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata
1	TBD	Modified to address Order No. 693 Directives contained in paragraph 693.	Revised.

1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Facility Ratings Methodology**

2. Number: FAC-008-1

3. Purpose: To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Transmission Owner

4.2. Generator Owner

5. Effective Date: August 7, 2006

B. Requirements

R1. The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:

R1.1. A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R1.2. The method by which the Rating (of major BES equipment that comprises a Facility) is determined.

R1.2.1. The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

R1.2.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R1.3. Consideration of the following:

R1.3.1. Ratings provided by equipment manufacturers.

R1.3.2. Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).

R1.3.3. Ambient conditions.

R1.3.4. Operating limitations.

R1.3.5. Other assumptions.

R2. The Transmission Owner and Generator Owner shall each make its Facility Ratings Methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners, and Planning Authorities that have responsibility for the area in which the associated Facilities are located, within 15 business days of receipt of a request. (Retired)

R3. If a Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides written comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall provide a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the

Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

C. Measures

M1. The Transmission Owner and Generator Owner shall each have a documented Facility Ratings Methodology that includes all of the items identified in FAC-008 Requirement 1.1 through FAC-008 Requirement 1.3.5.

M2. The Transmission Owner and Generator Owner shall each have evidence it made its Facility Ratings Methodology available for inspection within 15 business days of a request as follows: (Retired)

M2.1 The Reliability Coordinator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Reliability Coordinator Area. (Retired)

M2.2 The Transmission Operator shall have access to the Facility Ratings Methodologies used for Rating Facilities in its portion of the Reliability Coordinator Area. (Retired)

M2.3 The Transmission Planner shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Transmission Planning Area. (Retired)

M2.4 The Planning Authority shall have access to the Facility Ratings Methodologies used for Rating Facilities in its Planning Authority Area. (Retired)

M3. If the Reliability Coordinator, Transmission Operator, Transmission Planner, or Planning Authority provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings Methodology, the Transmission Owner or Generator Owner shall have evidence that it provided a written response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings Methodology and, if no change will be made to that Facility Ratings Methodology, the reason why. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Transmission Owner and Generator Owner shall self-certify its compliance to the Compliance Monitor at least once every three years. New Transmission Owners and Generator Owners shall each demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

The Transmission Owner and Generator Owner shall each keep all superseded portions of its Facility Ratings Methodology for 12 months beyond the date of the change in that methodology and shall keep all documented comments on the Facility Ratings Methodology and associated responses for three years. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant.

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Transmission Owner and Generator Owner shall each make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 Facility Ratings Methodology

1.4.2 Superseded portions of its Facility Ratings Methodology that had been replaced, changed or revised within the past 12 months

1.4.3 Documented comments provided by a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Authority on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology, and the associated responses

2. Levels of Non-Compliance

2.1. Level 1: There shall be a level one non-compliance if any of the following conditions exists:

2.1.1 The Facility Ratings Methodology does not contain a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.1.2 The Facility Ratings Methodology does not address one of the required equipment types identified in FAC-008 R1.2.1.

2.1.3 No evidence of responses to a Reliability Coordinator's, Transmission Operator, Transmission Planner, or Planning Authority's comments on the Facility Ratings Methodology. (Retired)

2.2. Level 2: The Facility Ratings Methodology is missing the assumptions used to determine Facility Ratings or does not address two of the required equipment types identified in FAC-008 R1.2.1.

2.3. Level 3: The Facility Ratings Methodology does not address three of the required equipment types identified in FAC-008-1 R1.2.1.

2.4. Level 4: The Facility Ratings Methodology does not address both Normal and Emergency Ratings ~~or the Facility Ratings Methodology was not made available for inspection within 15 business days of receipt of a request~~. (Deleted text retired)

E. Regional Differences

None Identified.

Version History

Version	Date	Action	Change Tracking
1	01/01/05	1. Lower cased the word "draft" and "drafting team" where appropriate. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Changed "Timeframe" to "Time	01/20/05

		Frame" and "twelve" to "12" in item D, 1.2.	
1	TBD	R2 and R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Facility Ratings**

2. **Number:** FAC-008-3

3. **Purpose:** To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits.

4. **Applicability**

   4.1. Transmission Owner.

   4.2. Generator Owner.

5. **Effective Date:** The first day of the first calendar quarter that is twelve months beyond the date approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the first day of the first calendar quarter twelve months following BOT adoption.

B. Requirements

R1. Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

1.1. The documentation shall contain assumptions used to rate the generator and at least one of the following:

- Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis.
- Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses.

1.2. The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

R2. Each Generator Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned equipment connected between the location specified in R1 and the point of interconnection with the Transmission Owner that contains all of the following. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

2.1. The methodology used to establish the Ratings of the equipment that comprises the Facility(ies) shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

- One or more industry standards developed through an open process such as Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

2.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R2, Part 2.1 including identification of how each of the following were considered:

2.2.1. Equipment Rating standard(s) used in development of this methodology.

2.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

2.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

2.2.4. Operating limitations.[1]

2.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

2.4. The process by which the Rating of equipment that comprises a Facility is determined.

2.4.1. The scope of equipment addressed shall include, but not be limited to, conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

2.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R3. Each Transmission Owner shall have a documented methodology for determining Facility Ratings (Facility Ratings methodology) of its solely and jointly owned Facilities (except for those generating unit Facilities addressed in R1 and R2) that contains all of the following: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:

- Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.
- One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
- A practice that has been verified by testing, performance history or engineering analysis.

3.2. The underlying assumptions, design criteria, and methods used to determine the Equipment Ratings identified in Requirement R3, Part 3.1 including identification of how each of the following were considered:

3.2.1. Equipment Rating standard(s) used in development of this methodology.

[1] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

3.2.2. Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications.

3.2.3. Ambient conditions (for particular or average conditions or as they vary in real-time).

3.2.4. Operating limitations.[2]

3.3. A statement that a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.

3.4. The process by which the Rating of equipment that comprises a Facility is determined.

3.4.1. The scope of equipment addressed shall include, but not be limited to, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.

3.4.2. The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.

R4. Each Transmission Owner shall make its Facility Ratings methodology and each Generator Owner shall each make its documentation for determining its Facility Ratings and its Facility Ratings methodology available for inspection and technical review by those Reliability Coordinators, Transmission Operators, Transmission Planners and Planning Coordinators that have responsibility for the area in which the associated Facilities are located, within 21 calendar days of receipt of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R5. If a Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's Facility Ratings methodology or Generator Owner's documentation for determining its Facility Ratings and its Facility Rating methodology, the Transmission Owner or Generator Owner shall provide a response to that commenting entity within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Facility Ratings methodology and, if no change will be made to that Facility Ratings methodology, the reason why. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* (Retired)

R6. Each Transmission Owner and Generator Owner shall have Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology or documentation for determining its Facility Ratings. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R7. Each Generator Owner shall provide Facility Ratings (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) as scheduled by such requesting entities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R8. Each Transmission Owner (and each Generator Owner subject to Requirement R2) shall provide requested information as specified below (for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities) to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

[2] Such as temporary de-ratings of impaired equipment in accordance with good utility practice.

8.1. As scheduled by the requesting entities:

8.1.1. Facility Ratings

8.1.2. Identity of the most limiting equipment of the Facilities

8.2. Within 30 calendar days (or a later date if specified by the requester), for any requested Facility with a Thermal Rating that limits the use of Facilities under the requester's authority by causing any of the following: 1) An Interconnection Reliability Operating Limit, 2) A limitation of Total Transfer Capability, 3) An impediment to generator deliverability, or 4) An impediment to service to a major load center:

8.2.1. Identity of the existing next most limiting equipment of the Facility

8.2.2. The Thermal Rating for the next most limiting equipment identified in Requirement R8, Part 8.2.1.

C. Measures

M1. Each Generator Owner shall have documentation that shows how its Facility Ratings were determined as identified in Requirement 1.

M2. Each Generator Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 2, Parts 2.1 through 2.4.

M3. Each Transmission Owner shall have a documented Facility Ratings methodology that includes all of the items identified in Requirement 3, Parts 3.1 through 3.4.

M4. Each Transmission Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement 4. The Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it made its documentation for determining its Facility Ratings or its Facility Ratings methodology available for inspection within 21 calendar days of a request in accordance with Requirement R4. (Retired)

M5. If the Reliability Coordinator, Transmission Operator, Transmission Planner or Planning Coordinator provides documented comments on its technical review of a Transmission Owner's or Generator Owner's Facility Ratings methodology or a Generator Owner's documentation for determining its Facility Ratings, the Transmission Owner or Generator Owner shall have evidence, (such as a copy of a dated electronic or hard copy note, or other comparable evidence from the Transmission Owner or Generator Owner addressed to the commenter that includes the response to the comment,) that it provided a response to that commenting entity in accordance with Requirement R5. (Retired)

M6. Each Transmission Owner and Generator Owner shall have evidence to show that its Facility Ratings are consistent with the documentation for determining its Facility Ratings as specified in Requirement R1 or consistent with its Facility Ratings methodology as specified in Requirements R2 and R3 (Requirement R6).

M7. Each Generator Owner shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings to its associated Reliability Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R7.

M8. Each Transmission Owner (and Generator Owner subject to Requirement R2) shall have evidence, such as a copy of a dated electronic note, or other comparable evidence to show that it provided its Facility Ratings and identity of limiting equipment to its associated Reliability

Coordinator(s), Planning Coordinator(s), Transmission Planner(s), Transmission Owner(s) and Transmission Operator(s) in accordance with Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Compliance Monitoring and Enforcement Processes:

- Self-Certifications
- Spot Checking
- Compliance Audits
- Self-Reporting
- Compliance Violation Investigations
- Complaints

1.3. Data Retention

The Generator Owner shall keep its current documentation (for R1) and any modifications to the documentation that were in force since last compliance audit period for Measure M1 and Measure M6.

The Generator Owner shall keep its current, in force Facility Ratings methodology (for R2) and any modifications to the methodology that were in force since last compliance audit period for Measure M2 and Measure M6.

The Transmission Owner shall keep its current, in force Facility Ratings methodology (for R3) and any modifications to the methodology that were in force since the last compliance audit for Measure M3 and Measure M6.

The Transmission Owner and Generator Owner shall keep its current, in force Facility Ratings and any changes to those ratings for three calendar years for Measure M6.

The Generator Owner and Transmission Owner shall each keep evidence for Measure M4, and Measure M5, for three calendar years. (Retired)

The Generator Owner shall keep evidence for Measure M7 for three calendar years.

The Transmission Owner (and Generator Owner that is subject to Requirement R2) shall keep evidence for Measure M8 for three calendar years.

If a Generator Owner or Transmission Owner is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

None

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	• The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.1.	The Generator Owner's Facility Rating documentation did not address Requirement R1, Part 1.2.	The Generator Owner failed to provide documentation for determining its Facility Ratings.
R2	The Generator Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology did not address all the components of Requirement R2, Part 2.4. OR The Generator Owner failed to include in its Facility Rating Methodology, three of the following Parts of Requirement R2: • 2.1. • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4	The Generator Owner's Facility Rating methodology failed to recognize a facility's rating based on the most limiting component rating as required in Requirement R2, Part 2.3 OR The Generator Owner failed to include in its Facility Rating Methodology four or more of the following Parts of Requirement R2: • 2.1 • 2.2.1 • 2.2.2 • 2.2.3 • 2.2.4
R3	The Transmission Owner failed to include in its Facility Rating methodology one of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner failed to include in its Facility Rating methodology two of the following Parts of Requirement R3: • 3.1 • 3.2.1	The Transmission Owner's Facility Rating methodology did not address either of the following Parts of Requirement R3: • 3.4.1 • 3.4.2	The Transmission Owner's Facility Rating methodology failed to recognize a Facility's rating based on the most limiting component rating as required in Requirement R3, Part 3.3 OR

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	• 3.2.2 • 3.2.3 • 3.2.4	• 3.2.2 • 3.2.3 • 3.2.4	OR The Transmission Owner failed to include in its Facility Rating methodology three of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4	The Transmission Owner failed to include in its Facility Rating methodology four or more of the following Parts of Requirement R3: • 3.1 • 3.2.1 • 3.2.2 • 3.2.3 • 3.2.4
R4 (Retired)	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 21 calendar days but less than or equal to 31 calendar days after a request.	The responsible entity made its Facility Ratings methodology or Facility Ratings documentation available within more than 31 calendar days but less than or equal to 41 calendar days after a request.	The responsible entity made its Facility Rating methodology or Facility Ratings documentation available within more than 41 calendar days but less than or equal to 51 calendar days after a request.	The responsible entity failed to make its Facility Ratings methodology or Facility Ratings documentation available in more than 51 calendar days after a request. (R3)
R5 (Retired)	The responsible entity provided a response in more than 45 calendar days but less than or equal to 60 calendar days after a request. (R5)	The responsible entity provided a response in more than 60 calendar days but less than or equal to 70 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, and the response indicated that a change will not be made to the Facility Ratings methodology or Facility Ratings documentation but did not indicate why no change will be made. (R5)	The responsible entity provided a response in more than 70 calendar days but less than or equal to 80 calendar days after a request. OR The responsible entity provided a response within 45 calendar days, but the response did not indicate whether a change will be made to the Facility Ratings methodology or Facility Ratings documentation. (R5)	The responsible entity failed to provide a response as required in more than 80 calendar days after the comments were received. (R5)

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for 5% or less of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 5% or more, but less than up to (and including) 10% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than 10% up to (and including) 15% of its solely owned and jointly owned Facilities. (R6)	The responsible entity failed to establish Facility Ratings consistent with the associated Facility Ratings methodology or documentation for determining the Facility Ratings for more than15% of its solely owned and jointly owned Facilities. (R6)
R7	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days.	The Generator Owner provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. OR The Generator Owner failed to provide its Facility Ratings to the requesting entities.
R8	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by up to and including 15 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to all of the requesting entities. (R8, Part 8.1)	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 15 calendar days but less than or equal to 25 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 25 calendar days but less than or equal to 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 90%, but not less than or equal to 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR	The responsible entity provided its Facility Ratings to all of the requesting entities but missed meeting the schedules by more than 35 calendar days. (R8, Part 8.1) OR The responsible entity provided less than 85% of the required Rating information to all of the requesting entities. (R8, Part 8.1) OR The responsible entity provided the required Rating information to the requesting entity, but did so more

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The responsible entity provided the required Rating information to the requesting entity, but the information was provided up to and including 15 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 100%, but not less than or equal to 95% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more 15 calendar days but less than or equal to 25 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 95%, but not less than or equal to 90% of the required Rating information to the requesting entity. (R8, Part 8.2)	The responsible entity provided the required Rating information to the requesting entity, but did so more than 25 calendar days but less than or equal to 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 90%, but no less than or equal to 85% of the required Rating information to the requesting entity. (R8, Part 8.2)	than 35 calendar days late. (R8, Part 8.2) OR The responsible entity provided less than 85 % of the required Rating information to the requesting entity. (R8, Part 8.2) OR The responsible entity failed to provide its Rating information to the requesting entity. (R8, Part 8.1)

E. Regional Variances

None.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	Feb 7, 2006	Approved by Board of Trustees	New
1	Mar 16, 2007	Approved by FERC	New
2	May 12, 2010	Approved by Board of Trustees	Complete Revision, merging FAC_008-1 and FAC-009-1 under Project 2009-06 and address directives from Order 693
3	May 24, 2011	Addition of Requirement R8	Project 2009-06 Expansion to address third directive from Order 693
3	May 24, 2011	Adopted by NERC Board of Trustees	
3	November 17, 2011	FERC Order issued approving FAC-008-3	
3	May 17, 2012	FERC Order issued directing the VRF for Requirement R2 be changed from “Lower” to “Medium”	
3	TBD	R4 and R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Operating Limits Methodology for the Planning Horizon**

2. Number: FAC-010-2.1

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable planning of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Planning Authority

5. Effective Date: April 19, 2010

B. Requirements

R1. The Planning Authority shall have a documented SOL Methodology for use in developing SOLs within its Planning Authority Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the planning horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Planning Authority's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state and with all Facilities in service, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or three-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. Starting with all Facilities in service, the system's response to a single Contingency, may include any of the following:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R2.5. Starting with all Facilities in service and following any of the multiple Contingencies identified in Reliability Standard TPL-003 the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.6. In determining the system's response to any of the multiple Contingencies, identified in Reliability Standard TPL-003, in addition to the actions identified in R2.3.1 and R2.3.2, the following shall be acceptable:

R2.6.1. Planned or controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers.

R3. The Planning Authority's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Planning Authority Area as well as the critical modeling details from other Planning Authority Areas that would impact the Facility or Facilities under study).

R3.2. Selection of applicable Contingencies.

R3.3. Level of detail of system models used to determine SOLs.

R3.4. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.5. Anticipated transmission system configuration, generation dispatch and Load level.

R3.6. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.

R4. The Planning Authority shall issue its SOL Methodology, and any change to that methodology, to all of the following prior to the effectiveness of the change:

R4.1. Each adjacent Planning Authority and each Planning Authority that indicated it has a reliability-related need for the methodology.

R4.2. Each Reliability Coordinator and Transmission Operator that operates any portion of the Planning Authority's Planning Authority Area.

R4.3. Each Transmission Planner that works in the Planning Authority's Planning Authority Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Planning Authority shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. Measures

M1. The Planning Authority's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Planning Authority shall have evidence it issued its SOL Methodology and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Planning Authority that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Planning Authority shall self-certify its compliance to the Compliance Monitor at least once every three years. New Planning Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Planning Authority shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Planning Authority shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology. (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R2.1 through R2.3 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.2	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.3.	The Planning Authority has a documented SOL Methodology for use in developing SOLs within its Planning Authority Area, but it does not address R1.1. OR The Planning Authority has no documented SOL Methodology for use in developing SOLs within its Planning Authority Area.
R2	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance following single and multiple contingencies, but does not address the pre-contingency state (R2.1)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following single contingencies, but does not address multiple contingencies. (R2.5-R2.6)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state and following multiple contingencies, but does not meet the performance for response to single contingencies. (R2.2 –R2.4)	The Planning Authority's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state but does not require that SOLs be set to meet the BES performance specified for response to single contingencies (R2.2-R2.4) and does not require that SOLs be set to meet the BES performance specified for response to multiple contingencies. (R2.5-R2.6)
R3	The Planning Authority has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.6.	The Planning Authority has a methodology for determining SOLs that is missing a description of four or more of the following: R3.1 through R3.6.
R4	One or both of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority issued its SOL Methodology and changes	One of the following: The Planning Authority failed to issue its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to more than three of the required entities. The Planning Authority issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Planning Authority issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. The Planning Authority issued its SOL Methodology and changes to that methodology to all but

Requirement	Lower	Moderate	High	Severe
				four of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.
R5 (Retired)	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Planning Authority's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Planning Authority received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Planning Authority's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

E. Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-010.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
1	November 1, 2006	Fixed typo. Removed the word "each" from the 1st sentence of section D.1.3, Data Retention.	01/11/07
2	June 24, 2008	Adopted by Board of Trustees; FERC Order 705	Revised
2		Changed the effective date to July 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2.1	November 5, 2009	Adopted by the Board of Trustees — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	April 19, 2010	FERC Approved — errata change Section E1.1 modified to reflect the renumbering of requirements R2.4 and R2.5 from FAC-010-1 to R2.5 and R2.6 in FAC-010-2.	Errata
2.1	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **System Operating Limits Methodology for the Operations Horizon**

2. Number: FAC-011-2

3. Purpose: To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: April 29, 2009

B. Requirements

R1. The Reliability Coordinator shall have a documented methodology for use in developing SOLs (SOL Methodology) within its Reliability Coordinator Area. This SOL Methodology shall:

R1.1. Be applicable for developing SOLs used in the operations horizon.

R1.2. State that SOLs shall not exceed associated Facility Ratings.

R1.3. Include a description of how to identify the subset of SOLs that qualify as IROLs.

R2. The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages.

R2.2. Following the single Contingencies[1] identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur.

R2.2.1. Single line to ground or 3-phase Fault (whichever is more severe), with Normal Clearing, on any Faulted generator, line, transformer, or shunt device.

R2.2.2. Loss of any generator, line, transformer, or shunt device without a Fault.

R2.2.3. Single pole block, with Normal Clearing, in a monopolar or bipolar high voltage direct current system.

R2.3. In determining the system's response to a single Contingency, the following shall be acceptable:

R2.3.1. Planned or controlled interruption of electric supply to radial customers or some local network customers connected to or supplied by the Faulted Facility or by the affected area.

[1] The Contingencies identified in FAC-011 R2.2.1 through R2.2.3 are the minimum contingencies that must be studied but are not necessarily the only Contingencies that should be studied.

R2.3.2. Interruption of other network customers, (a) only if the system has already been adjusted, or is being adjusted, following at least one prior outage, or (b) if the real-time operating conditions are more adverse than anticipated in the corresponding studies

R2.3.3. System reconfiguration through manual or automatic control or protection actions.

R2.4. To prepare for the next Contingency, system adjustments may be made, including changes to generation, uses of the transmission system, and the transmission system topology.

R3. The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.1. Study model (must include at least the entire Reliability Coordinator Area as well as the critical modeling details from other Reliability Coordinator Areas that would impact the Facility or Facilities under study.)

R3.2. Selection of applicable Contingencies

R3.3. A process for determining which of the stability limits associated with the list of multiple contingencies (provided by the Planning Authority in accordance with FAC-014 Requirement 6) are applicable for use in the operating horizon given the actual or expected system conditions.

R3.3.1. This process shall address the need to modify these limits, to modify the list of limits, and to modify the list of associated multiple contingencies.

R3.4. Level of detail of system models used to determine SOLs.

R3.5. Allowed uses of Special Protection Systems or Remedial Action Plans.

R3.6. Anticipated transmission system configuration, generation dispatch and Load level

R3.7. Criteria for determining when violating a SOL qualifies as an Interconnection Reliability Operating Limit (IROL) and criteria for developing any associated IROL T_v.

R4. The Reliability Coordinator shall issue its SOL Methodology and any changes to that methodology, prior to the effectiveness of the Methodology or of a change to the Methodology, to all of the following:

R4.1. Each adjacent Reliability Coordinator and each Reliability Coordinator that indicated it has a reliability-related need for the methodology.

R4.2. Each Planning Authority and Transmission Planner that models any portion of the Reliability Coordinator's Reliability Coordinator Area.

R4.3. Each Transmission Operator that operates in the Reliability Coordinator Area.

R5. If a recipient of the SOL Methodology provides documented technical comments on the methodology, the Reliability Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the SOL Methodology and, if no change will be made to that SOL Methodology, the reason why. (Retired)

C. Measures

M1. The Reliability Coordinator's SOL Methodology shall address all of the items listed in Requirement 1 through Requirement 3.

M2. The Reliability Coordinator shall have evidence it issued its SOL Methodology, and any changes to that methodology, including the date they were issued, in accordance with Requirement 4.

M3. If the recipient of the SOL Methodology provides documented comments on its technical review of that SOL methodology, the Reliability Coordinator that distributed that SOL Methodology shall have evidence that it provided a written response to that commenter within 45 calendar days of receipt of those comments in accordance with Requirement 5 (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

Each Reliability Coordinator shall self-certify its compliance to the Compliance Monitor at least once every three years. New Reliability Authorities shall demonstrate compliance through an on-site audit conducted by the Compliance Monitor within the first year that it commences operation. The Compliance Monitor shall also conduct an on-site audit once every nine years and an investigation upon complaint to assess performance.

The Performance-Reset Period shall be twelve months from the last non-compliance.

1.3. Data Retention

The Reliability Coordinator shall keep all superseded portions to its SOL Methodology for 12 months beyond the date of the change in that methodology ~~and shall keep all documented comments on its SOL Methodology and associated responses for three years~~. In addition, entities found non-compliant shall keep information related to the non-compliance until found compliant. (Deleted text retired)

The Compliance Monitor shall keep the last audit and all subsequent compliance records.

1.4. Additional Compliance Information

The Reliability Coordinator shall make the following available for inspection during an on-site audit by the Compliance Monitor or within 15 business days of a request as part of an investigation upon complaint:

1.4.1 SOL Methodology.

1.4.2 Documented comments provided by a recipient of the SOL Methodology on its technical review of a SOL Methodology, and the associated responses. (Retired)

1.4.3 Superseded portions of its SOL Methodology that had been made within the past 12 months.

1.4.4 Evidence that the SOL Methodology and any changes to the methodology that occurred within the past 12 months were issued to all required entities.

2. Levels of Non-Compliance for Western Interconnection: (To be replaced with VSLs once developed and approved by WECC)

2.1. Level 1: There shall be a level one non-compliance if either of the following conditions exists:

2.1.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded.

2.1.2 No evidence of responses to a recipient's comments on the SOL Methodology (Retired)

2.2. Level 2: The SOL Methodology did not include a requirement to address all of the elements in R3.1, R3.2, R3.4 through R3.7 and E1.

2.3. Level 3: There shall be a level three non-compliance if any of the following conditions exists:

2.3.1 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to one of the three types of single Contingencies identified in R2.2.

2.3.2 The SOL Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not include evaluation of system response to two of the seven types of multiple Contingencies identified in E1.1.

2.3.3 The System Operating Limits Methodology did not include a statement indicating that Facility Ratings shall not be exceeded and the methodology did not address two of the six required topics in R3.1, R3.2, R3.4 through R3.7.

2.4. Level 4: The SOL Methodology was not issued to all required entities in accordance with R4.

3. Violation Severity Levels:

Requirement	Lower	Moderate	High	Severe
R1	Not applicable.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.2	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.3.	The Reliability Coordinator has a documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area, but it does not address R1.1. OR The Reliability Coordinator has no documented SOL Methodology for use in developing SOLs within its Reliability Coordinator Area.
R2	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance following single contingencies, but does not require that SOLs are set to meet BES performance in the pre-contingency state. (R2.1)	Not applicable.	The Reliability Coordinator's SOL Methodology requires that SOLs are set to meet BES performance in the pre-contingency state, but does not require that SOLs are set to meet BES performance following single contingencies. (R2.2 – R2.4)	The Reliability Coordinator's SOL Methodology does not require that SOLs are set to meet BES performance in the pre-contingency state and does not require that SOLs are set to meet BES performance following single contingencies. (R2.1 through R2.4)
R3	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but one of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but two of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that includes a description for all but three of the following: R3.1 through R3.7.	The Reliability Coordinator has a methodology for determining SOLs that is missing a description of three or more of the following: R3.1 through R3.7.
R4	One or both of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities. For a change in methodology, the changed methodology was	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 30	One of the following: The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 60	One of the following: The Reliability Coordinator failed to issue its SOL Methodology and changes to that methodology to more than three of the required entities. The Reliability Coordinator issued its SOL Methodology and

Requirement	Lower	Moderate	High	Severe
	provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided up to 30 calendar days after the effectiveness of the change.	changes to that methodology to all but one of the required entities AND for a change in methodology, the changed methodology was provided 90 calendar days or more after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but two of the required entities AND for a change in methodology, the changed methodology was provided 60 calendar days or more, but less than 90 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but three of the required entities AND for a change in methodology, the changed methodology was provided 30 calendar days or more, but less than 60 calendar days after the effectiveness of the change. OR The Reliability Coordinator issued its SOL Methodology and changes to that methodology to all but four of the required entities AND for a change in methodology, the changed methodology was provided up to

Requirement	Lower	Moderate	High	Severe
				30 calendar days after the effectiveness of the change.
R5 (Retired)	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was longer than 45 calendar days but less than 60 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 60 calendar days or longer but less than 75 calendar days.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 75 calendar days or longer but less than 90 calendar days. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology indicated that a change will not be made, but did not include an explanation of why the change will not be made.	The Reliability Coordinator received documented technical comments on its SOL Methodology and provided a complete response in a time period that was 90 calendar days or longer. OR The Reliability Coordinator's response to documented technical comments on its SOL Methodology did not indicate whether a change will be made to the SOL Methodology.

Regional Differences

1. The following Interconnection-wide Regional Difference shall be applicable in the Western Interconnection:

1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:

1.1.1 Simultaneous permanent phase to ground Faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with Normal Clearing. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded.

1.1.2 A permanent phase to ground Fault on any generator, transmission circuit, transformer, or bus section with Delayed Fault Clearing except for bus sectionalizing breakers or bus-tie breakers addressed in E1.1.7

1.1.3 Simultaneous permanent loss of both poles of a direct current bipolar Facility without an alternating current Fault.

1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.

1.1.5 A non-three phase Fault with Normal Clearing on common mode Contingency of two adjacent circuits on separate towers unless the event frequency is determined to be less than one in thirty years.

1.1.6 A common mode outage of two generating units connected to the same switchyard, not otherwise addressed by FAC-011.

1.1.7 The loss of multiple bus sections as a result of failure or delayed clearing of a bus tie or bus sectionalizing breaker to clear a permanent Phase to Ground Fault.

1.2. SOLs shall be established such that for multiple Facility Contingencies in E1.1.1 through E1.1.5 operation within the SOL shall provide system performance consistent with the following:

1.2.1 All Facilities are operating within their applicable Post-Contingency thermal, frequency and voltage limits.

1.2.2 Cascading does not occur.

1.2.3 Uncontrolled separation of the system does not occur.

1.2.4 The system demonstrates transient, dynamic and voltage stability.

1.2.5 Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall security of the interconnected transmission systems.

1.2.6 Interruption of firm transfer, Load or system reconfiguration is permitted through manual or automatic control or protection actions.

1.2.7 To prepare for the next Contingency, system adjustments are permitted, including changes to generation, Load and the transmission system topology when determining limits.

1.3. SOLs shall be established such that for multiple Facility Contingencies in E1.1.6 through E1.1.7 operation within the SOL shall provide system performance consistent with the following with respect to impacts on other systems:

1.3.1 Cascading does not occur.

1.4. The Western Interconnection may make changes (performance category adjustments) to the Contingencies required to be studied and/or the required responses to Contingencies for specific facilities based on actual system performance and robust design. Such changes will apply in determining SOLs.

Version History

Version	Date	Action	Change Tracking
1	November 1, 2006	Adopted by Board of Trustees	New
2		Changed the effective date to October 1, 2008 Changed "Cascading Outage" to "Cascading" Replaced Levels of Non-compliance with Violation Severity Levels Corrected footnote 1 to reference FAC-011 rather than FAC-010	Revised
2	June 24, 2008	Adopted by Board of Trustees: FERC Order 705	Revised
2	January 22, 2010	Updated effective date and footer to April 29, 2009 based on the March 20, 2009 FERC Order	Update
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

2. Number: FAC-013-2

3. Purpose: To ensure that Planning Coordinators have a methodology for, and perform an annual assessment to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliably transfer energy in the Near-Term Transmission Planning Horizon.

4. Applicability:

4.1. Planning Coordinators

5. Effective Date:

In those jurisdictions where regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after applicable regulatory approval or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-2 are effective.

In those jurisdictions where no regulatory approval is required, the latter of either the first day of the first calendar quarter twelve months after Board of Trustees adoption or the first day of the first calendar quarter six months after MOD-001-1, MOD-028-1, MOD-029-1 and MOD-030-2 are effective.

B. Requirements

R1. Each Planning Coordinator shall have a documented methodology it uses to perform an annual assessment of Transfer Capability in the Near-Term Transmission Planning Horizon (Transfer Capability methodology). The Transfer Capability methodology shall include, at a minimum, the following information: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Criteria for the selection of the transfers to be assessed.

1.2. A statement that the assessment shall respect known System Operating Limits (SOLs).

1.3. A statement that the assumptions and criteria used to perform the assessment are consistent with the Planning Coordinator's planning practices.

1.4. A description of how each of the following assumptions and criteria used in performing the assessment are addressed:

1.4.1. Generation dispatch, including but not limited to long term planned outages, additions and retirements.

1.4.2. Transmission system topology, including but not limited to long term planned Transmission outages, additions, and retirements.

1.4.3. System demand.

1.4.4. Current approved and projected Transmission uses.

1.4.5. Parallel path (loop flow) adjustments.

1.4.6. Contingencies

1.4.7. Monitored Facilities.

1.5. A description of how simulations of transfers are performed through the adjustment of generation, Load or both.

R2. Each Planning Coordinator shall issue its Transfer Capability methodology, and any revisions to the Transfer Capability methodology, to the following entities subject to the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

2.1. Distribute to the following prior to the effectiveness of such revisions:

2.1.1. Each Planning Coordinator adjacent to the Planning Coordinator's Planning Coordinator area or overlapping the Planning Coordinator's area.

2.1.2. Each Transmission Planner within the Planning Coordinator's Planning Coordinator area.

2.2. Distribute to each functional entity that has a reliability-related need for the Transfer Capability methodology and submits a request for that methodology within 30 calendar days of receiving that written request.

R3. If a recipient of the Transfer Capability methodology provides documented concerns with the methodology, the Planning Coordinator shall provide a documented response to that recipient within 45 calendar days of receipt of those comments. The response shall indicate whether a change will be made to the Transfer Capability methodology and, if no change will be made to that Transfer Capability methodology, the reason why. *[Violation Risk Factor: Lower][Time Horizon: Long-term Planning]* (Retired)

R4. During each calendar year, each Planning Coordinator shall conduct simulations and document an assessment based on those simulations in accordance with its Transfer Capability methodology for at least one year in the Near-Term Transmission Planning Horizon. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

R5. Each Planning Coordinator shall make the documented Transfer Capability assessment results available within 45 calendar days of the completion of the assessment to the recipients of its Transfer Capability methodology pursuant to Requirement R2, Parts 2.1 and Part 2.2. However, if a functional entity that has a reliability related need for the results of the annual assessment of the Transfer Capabilities makes a written request for such an assessment after the completion of the assessment, the Planning Coordinator shall make the documented Transfer Capability assessment results available to that entity within 45 calendar days of receipt of the request *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

R6. If a recipient of a documented Transfer Capability assessment requests data to support the assessment results, the Planning Coordinator shall provide such data to that entity within 45 calendar days of receipt of the request. The provision of such data shall be subject to the legal and regulatory obligations of the Planning Coordinator's area regarding the disclosure of confidential and/or sensitive information. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

C. Measures

M1. Each Planning Coordinator shall have a Transfer Capability methodology that includes the information specified in Requirement R1.

M2. Each Planning Coordinator shall have evidence such as dated e-mail or dated transmittal letters that it provided the new or revised Transfer Capability methodology in accordance with Requirement R2

M3. Each Planning Coordinator shall have evidence, such as dated e-mail or dated transmittal letters, that the Planning Coordinator provided a written response to that commenter in accordance with Requirement R3. (Retired)

M4. Each Planning Coordinator shall have evidence such as dated assessment results, that it conducted and documented a Transfer Capability assessment in accordance with Requirement R4.

M5. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment available to the entities in accordance with Requirement R5.

M6. Each Planning Coordinator shall have evidence, such as dated copies of e-mails or transmittal letters, that it made its documented Transfer Capability assessment data available in accordance with Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Data Retention

The Planning Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- The Planning Coordinator shall have its current Transfer Capability methodology and any prior versions of the Transfer Capability methodology that were in force since the last compliance audit to show compliance with Requirement R1.
- The Planning Coordinator shall retain evidence since its last compliance audit to show compliance with Requirement R2.
- The Planning Coordinator shall retain evidence to show compliance with Requirements R3, R4, R5 and R6 for the most recent assessment. (R3 retired)
- If a Planning Coordinator is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time periods specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Planning Coordinator has a Transfer Capability methodology but failed to address one or two of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address three of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate two of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address four of the items listed in Requirement R1, Part 1.4.	The Planning Coordinator did not have a Transfer Capability methodology. OR The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate three or more of the following Parts of Requirement R1 into that methodology: • Part 1.1 • Part 1.2 • Part 1.3 • Part 1.5 OR The Planning Coordinator has a Transfer Capability methodology but failed to address more than four of the items listed in Requirement R1, Part 1.4.

R2	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology after its implementation, but not more than 30 calendar days after its implementation. OR The Planning Coordinator provided the transfer Capability methodology more than 30 calendar days but not more than 60 calendar days after the receipt of a request.	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 30 calendar days after its implementation, but not more than 60 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 60 calendar days but not more than 90 calendar days after receipt of a request	The Planning Coordinator notified one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 60 calendar days, but not more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 90 calendar days but not more than 120 calendar days after receipt of a request.	The Planning Coordinator failed to notify one or more of the parties specified in Requirement R2 of a new or revised Transfer Capability methodology more than 90 calendar days after its implementation. OR The Planning Coordinator provided the Transfer Capability methodology more than 120 calendar days after receipt of a request.
R3 **(Retired)**	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 45 calendar days, but not more than 60 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 60 calendar days, but not more than 75 calendar days after receipt of the concern.	The Planning Coordinator provided a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 more than 75 calendar days, but not more than 90 calendar days after receipt of the concern.	The Planning Coordinator failed to provide a documented response to a documented concern with its Transfer Capability methodology as required in Requirement R3 by more than 90 calendar days after receipt of the concern. OR The Planning Coordinator failed to respond to a documented concern with its Transfer Capability methodology.

R4.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, but not by more than 30 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 30 calendar days, but not by more than 60 calendar days.	The Planning Coordinator conducted a Transfer Capability assessment outside the calendar year, by more than 60 calendar days, but not by more than 90 calendar days.	The Planning Coordinator failed to conduct a Transfer Capability assessment outside the calendar year by more than 90 calendar days. OR The Planning Coordinator failed to conduct a Transfer Capability assessment.

R5	The Planning Coordinator made its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 45 calendar days after the requirements of R5,, but not more than 60 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 60 calendar days after the requirements of R5, but not more than 75 calendar days after completion of the assessment.	The Planning Coordinator made its Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 75 calendar days after the requirements of R5, but not more than 90 days after completion of the assessment.	The Planning Coordinator failed to make its documented Transfer Capability assessment available to one or more of the recipients of its Transfer Capability methodology more than 90 days after the requirements of R5. OR The Planning Coordinator failed to make its documented Transfer Capability assessment available to any of the recipients of its Transfer Capability methodology under the requirements of R5.
R6	The Planning Coordinator provided the requested data as required in Requirement R6 more than 45 calendar days after receipt of the request for data, but not more than 60 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 60 calendar days after receipt of the request for data, but not more than 75 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 75 calendar days after receipt of the request for data, but not more than 90 calendar days after the receipt of the request for data.	The Planning Coordinator provided the requested data as required in Requirement R6 more than 90 after the receipt of the request for data. OR The Planning Coordinator failed to provide the requested data as required in Requirement R6.

E. **Regional Variances**

None.

F. **Associated Documents**

Version History

Version	Date	Action	Change Tracking
1	08/01/05	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Lower cased the word "draft" and "drafting team" where appropriate. 3. Changed Anticipated Action #5, page 1, from "30-day" to "Thirty-day." 4. Added or removed "periods."	01/20/05
2	01/24/11	Approved by BOT	
2	11/17/11	FERC Order issued approving FAC-013-2	
2	5/17/12	FERC Order issued directing the VRF's for Requirements R1. and R4. be changed from "Lower" to "Medium." FERC Order issued correcting the High and Severe VSL language for R1.	
2	TBD	R3 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Interchange Confirmation**

2. Number: **INT-007-1**

3. Purpose: To ensure that each Arranged Interchange is checked for reliability before it is implemented.

4. Applicability

4.1. Interchange Authority.

5. Effective Date: January 1, 2007

B. Requirements

R1. The Interchange Authority shall verify that Arranged Interchange is balanced and valid prior to transitioning Arranged Interchange to Confirmed Interchange by verifying the following:

R1.1. Source Balancing Authority megawatts equal sink Balancing Authority megawatts (adjusted for losses, if appropriate).

R1.2. All reliability entities involved in the Arranged Interchange are currently in the NERC registry. (Retired)

R1.3. The following are defined:

R1.3.1. Generation source and load sink.

R1.3.2. Megawatt profile.

R1.3.3. Ramp start and stop times.

R1.3.4. Interchange duration.

R1.4. Each Balancing Authority and Transmission Service Provider that received the Arranged Interchange information from the Interchange Authority for reliability assessment has provided approval.

C. Measures

M1. For each Arranged Interchange, the Interchange Authority shall show evidence that it has verified the Arranged Interchange information prior to the dissemination of the Confirmed Interchange.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Time Frame

The Performance-Reset Period shall be twelve months from the last noncompliance to Requirement 1.

1.3. Data Retention

The Interchange Authority shall keep 90 days of historical data. The Compliance Monitor shall keep audit records for a minimum of three calendar years.

1.4. Additional Compliance Information

Each Interchange Authority shall demonstrate compliance to the Compliance Monitor within the first year that this standard becomes effective or the first year the entity commences operation by self-certification to the Compliance Monitor.

Subsequent to the initial compliance review, compliance may be:

1.4.1 Verified by audit at least once every three years.

1.4.2 Verified by spot checks in years between audits.

1.4.3 Verified by annual audits of noncompliant Interchange Authorities, until compliance is demonstrated.

1.4.4 Verified at any time as the result of a complaint. Complaints must be lodged within 60 days of the incident. Complaints will be evaluated by the Compliance Monitor.

Each Interchange Authority shall make the following available for inspection by the Compliance Monitor upon request:

1.4.5 For compliance audits and spot checks, relevant data and system log records for the audit period which indicate an Interchange Authority's verification that all Arranged Interchange was balanced and valid as defined in R1. The Compliance Monitor may request up to a three-month period of historical data ending with the date the request is received by the Interchange Authority.

1.4.6 For specific complaints, only those data and system log records associated with the specific Interchange event contained in the complaint which indicate an Interchange Authority's verification that an Arranged Interchange was balanced and valid as defined in R1 for that specific Interchange

2. Levels of Non-Compliance

2.1. Level 1: One occurrence[1] where Interchange-related data was not verified as defined in R1.

2.2. Level 2: Two occurrences where Interchange-related data was not verified as defined in R1.

2.3. Level 3: Three occurrences where Interchange-related data was not verified as defined in R1.

2.4. Level 4: Four or more occurrences where Interchange-related data was not verified as defined in R1.

E. Regional Differences

None

[1] This does not include instances of not verifying due to extenuating circumstances approved by the Compliance Monitor.

Version History

Version	Date	Action	Change Tracking
1	TBD	R1.2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Coordination of Real-time Activities Between Reliability Coordinators**

2. Number: **IRO-016-1**

3. Purpose: To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.

4. Applicability

4.1. Reliability Coordinator

5. Effective Date: November 1, 2006

B. Requirements

R1. The Reliability Coordinator that identifies a potential, expected, or actual problem that requires the actions of one or more other Reliability Coordinators shall contact the other Reliability Coordinator(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.

R1.1. If the involved Reliability Coordinators agree on the problem and the actions to take to prevent or mitigate the system condition, each involved Reliability Coordinator shall implement the agreed-upon solution, and notify the involved Reliability Coordinators of the action(s) taken.

R1.2. If the involved Reliability Coordinators cannot agree on the problem(s) each Reliability Coordinator shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.).

R1.2.1. If time permits, this re-evaluation shall be done before taking corrective actions.

R1.2.2. If time does not permit, then each Reliability Coordinator shall operate as though the problem(s) exist(s) until the conflicting system status is resolved.

R1.3. If the involved Reliability Coordinators cannot agree on the solution, the more conservative solution shall be implemented.

R2. The Reliability Coordinator shall document (via operator logs or other data sources) its actions taken for either the event or for the disagreement on the problem(s) or for both. (Retired)

C. Measures

M1. For each event that requires Reliability Coordinator-to-Reliability Coordinator coordination, each involved Reliability Coordinator shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Time Frame

The performance reset period shall be one calendar year.

1.3. Data Retention

The Reliability Coordinator shall keep auditable evidence for a rolling 12 months. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance, whichever is longer.

1.4. Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction's discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Coordinators (the Reliability Coordinator that complained as well as the Reliability Coordinator that was investigated) within 45 days after the start of the investigation. As part of an audit or investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been coordinating actions to prevent or resolve potential, expected, or actual problems that adversely impact the Interconnection.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:

1.4.1 Evidence (operator log or other data source) to show coordination with other Reliability Coordinators.

2. Levels of Non-Compliance

2.1. Level 1: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did coordinate, but did not have evidence that it coordinated with other Reliability Coordinators.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: For potential, actual or expected events which required Reliability Coordinator-to-Reliability Coordinator coordination, the Reliability Coordinator did not coordinate with other Reliability Coordinators.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
Version 1	August 10, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash (–)." 2. Hyphenated "30-day" and "Reliability Coordinator-to-Reliability Coordinator" when used as adjective.	01/20/06

		3. Changed standard header to be consistent with standard "Title." 4. Added "periods" to items where appropriate. 5. Initial capped heading "Definitions of Terms Used in Standard." 6. Changed "Timeframe" to "Time Frame" in item D, 1.2. 7. Lower cased all words that are not "defined" terms — drafting team, and self-certification. 8. Changed apostrophes to "smart" symbols. 9. Removed comma after word "condition" in item R.1.1. 10. Added comma after word "expected" in item 1.4, last sentence. 11. Removed extra spaces between words where appropriate.	
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Nuclear Plant Interface Coordination**

2. Number: NUC-001-2

3. Purpose: This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. Applicability:

4.1. Nuclear Plant Generator Operator.

4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

4.2.1 Transmission Operators.

4.2.2 Transmission Owners.

4.2.3 Transmission Planners.

4.2.4 Transmission Service Providers.

4.2.5 Balancing Authorities.

4.2.6 Reliability Coordinators.

4.2.7 Planning Coordinators.

4.2.8 Distribution Providers.

4.2.9 Load-serving Entities.

4.2.10 Generator Owners.

4.2.11 Generator Operators.

5. Effective Date: April 1, 2010

B. Requirements

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Medium*]

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

R4.1. Incorporate the NPIRs into their operating analyses of the electric system.

R4.2. Operate the electric system to meet the NPIRs.

R4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

R5. The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]

R9.1. Administrative elements: (Retired)

R9.1.1. Definitions of key terms used in the agreement. (Retired)

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. (Retired)

R9.1.3. A requirement to review the agreement(s) at least every three years. (Retired)

R9.1.4. A dispute resolution mechanism. (Retired)

R9.2. Technical requirements and analysis:

R9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

R9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

R9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

R9.3. Operations and maintenance coordination:

R9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

R9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

R9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

R9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

R9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. .

R9.3.6. Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

R9.3.7. Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

R9.4. Communications and training:

R9.4.1. Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

R9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

R9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

R9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

R9.4.5. Provisions for personnel training, as related to NPIRs.

C. Measures

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. (Requirement 2 and 9)

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:

M4.1 The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)

M4.2 The electric system was operated to meet the NPIRs. (Requirement 4.2)

M4.3 The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)

M8. The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

2.1. Lower: Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.

2.2. Moderate: Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.

2.3. High: One or more requirements of R3 through R8 were not met.

2.4. Severe: No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

E. Regional Differences

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs.
Therefore the definition of NPLR for Canadian CANDU units will be as follows:

Nuclear Plant Licensing Requirements (NPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	Revision
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update
2	TBD	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. Title: **Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.**

2. Number: PRC-010-0

3. Purpose: Provide System preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program.

4. Applicability:

4.1. Load-Serving Entity that operates a UVLS program

4.2. Transmission Owner that owns a UVLS program

4.3. Transmission Operator that operates a UVLS program

4.4. Distribution Provider that owns or operates a UVLS program

5. Effective Date: April 1, 2005

B. Requirements

R1. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).

R1.1. This assessment shall include, but is not limited to:

R1.1.1. Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.

R1.1.2. Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.

R1.1.3. A review of the voltage set points and timing.

R2. The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days). (Retired)

C. Measures

M1. Each Transmission Owner's and Distribution Provider's UVLS program shall include the elements identified in Reliability Standard PRC-010-0_R1.

M2. Each Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall have evidence it provided documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC as specified in Reliability Standard PRC-010-0_R2. (Retired)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations. Each Regional Reliability Organization shall report compliance and violations to NERC via the NERC Compliance Reporting process.

1.2. Compliance Monitoring Period and Reset Timeframe

Assessments every five years or as required by System changes.

Current assessment on request (30 calendar days.)

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: An assessment of the UVLS program did not address one of the three requirements listed in Reliability Standard PRC-010-0_R1.1 or an assessment of the UVLS program was not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

Standard PRC-022-1 — Under-Voltage Load Shedding Program Performance

A. Introduction

1. **Title:** **Under-Voltage Load Shedding Program Performance**

2. **Number:** **PRC-022-1**

3. **Purpose:** Ensure that Under Voltage Load Shedding (UVLS) programs perform as intended to mitigate the risk of voltage collapse or voltage instability in the Bulk Electric System (BES).

4. **Applicability**

   4.1. Transmission Operator that operates a UVLS program.

   4.2. Distribution Provider that operates a UVLS program.

   4.3. Load-Serving Entity that operates a UVLS program.

5. **Effective Date:** May 1, 2006

B. Requirements

R1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:

R1.1. A description of the event including initiating conditions.

R1.2. A review of the UVLS set points and tripping times.

R1.3. A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.

R1.4. A summary of the findings.

R1.5. For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.

R2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request. (Retired)

C. Measures

M1. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have documentation of its analysis of UVLS operations and Misoperations in accordance with Requirement 1.1 through 1.5.

M2. Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall have evidence that it provided documentation of its analysis of UVLS program performance within 90 calendar days of a request by the Regional Reliability Organization. (Retired)

D. Compliance

1. Compliance Monitoring Process

   1.1. Compliance Monitoring Responsibility

   Regional Reliability Organization.

   1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall retain documentation of its analyses of UVLS operations and Misoperations for two years. The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

Transmission Operator, Load-Serving Entity, and Distribution Provider shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: Documentation of the analysis of UVLS performance was provided but did not include one of the five requirements in R1.

2.3. Level 3: Documentation of the analysis of UVLS performance was provided but did not include two or more of the five requirements in R1.

2.4. Level 4: Documentation of the analysis of UVLS performance was not provided.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	December 1, 2005	1. Removed comma after 2004 in "Development Steps Completed," #1. 2. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 3. Lower cased the word "region," "board," and "regional" throughout document where appropriate. 4. Added or removed "periods" where appropriate. 5. Changed "Timeframe" to "Time Frame" in item D, 1.2.	January 20, 2006
1	TBD	R2 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

A. Introduction

1. **Title:** **Voltage and Reactive Control**

2. **Number:** VAR-001-2

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators.

   4.2. Purchasing-Selling Entities.

   4.3. Load Serving Entities.

5. **(Proposed) Effective Date:** The first day of the first calendar quarter six months after applicable regulatory approval; or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after Board of Trustees' adoption.

B. Requirements

R1. Each Transmission Operator, individually and jointly with other Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboring Transmission Operators.

R2. Each Transmission Operator shall acquire sufficient reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – within its area to protect the voltage levels under normal and Contingency conditions. This includes the Transmission Operator's share of the reactive requirements of interconnecting transmission circuits.

R3. The Transmission Operator shall specify criteria that exempts generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.

R3.1. Each Transmission Operator shall maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule.

R3.2. For each generator that is on this exemption list, the Transmission Operator shall notify the associated Generator Owner.

R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule [1] at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).

R5. Each Purchasing-Selling Entity and Load Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to satisfy its reactive requirements identified by its Transmission Service Provider. (Retired)

[1] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

R6. The Transmission Operator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers.

R6.1. When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.

R7. The Transmission Operator shall be able to operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow.

R8. Each Transmission Operator shall operate or direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits.

R9. Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load– to support its voltage under first Contingency conditions.

R9.1. Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.

R10. Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.

R11. After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

R12. The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

C. Measures

M1. The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule as specified in Requirement 4 to each Generator Operator it requires to follow such a schedule.

M2. The Transmission Operator shall have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3.2.

M3. The Transmission Operator shall have evidence to show that it issued directives as specified in Requirement 6.1 when notified by a Generator Operator of the loss of an automatic voltage regulator control.

M4. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with Requirement 11.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months.

The Compliance Monitor shall retain any audit data for three years.

1.5. Additional Compliance Information

The Transmission Operator shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Violation Severity Levels (no changes)

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	TBD	Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised.
2	TBD	R5 and associated elements retired as part of the Paragraph 81 project (Project 2013-02)	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-02 Paragraph 81

Recirculation Ballot is now open through 8 p.m. Thursday, January 17, 2013

Now Available

A recirculation ballot window for the 20 standards with 36 requirements being proposed for retirement in this project is now open through **8 p.m. Eastern on Thursday, January 17, 2013**.

The following documents are posted on the project page for review and balloting:

- **Redline of Standards with Proposed Retirements** – A PDF document containing a redline of each of the affected standards, indicating the requirements and associated elements proposed to be retired with a "(Retired)" and with the version number remaining the same. When these Requirements are retired, the version numbers of the standards will NOT be incremented. After evaluating the options and consulting with the Standards Committee and Standards Committee Process Subcommittee, the P81 drafting team determined that this was the most practical approach. Incrementing the version numbers of each standard is impractical because, in some cases, a subsequent version has already been developed. In addition, incrementing the version would require renumbering Requirements where a retired Requirement created a gap in numbering, and this creates an undesirable administrative burden for entities using certain systems to manage their compliance programs.
- **Implementation Plan** – The implementation plan for retiring the Phase I requirements.

After considering stakeholder comments from the formal comment period and initial ballot that ended on December 10, 2012, the drafting team made some minor clarifying changes to the technical white paper. Additionally, CIP-001-2a R4 and EOP-004-1 R1 were moved to the 'Informational Purposes Only' section in the technical paper, as EOP-004-2 has been filed with regulatory authorities and the EOP-004-2 implementation plan calls for the retirement of CIP-001-2a R4 and EOP-004-1 R1.

Instructions

In the recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the recirculation ballot.

Members of the ballot pool associated with this project may log in and submit their vote for the standard by clicking here.

Next Steps

Voting results will be posted and announced after the ballot window closes. If approved, the standards with requirements being proposed for retirement will be submitted to the Board of Trustees and then filed with the appropriate regulatory authorities.

Background

On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated the following in P81:

> "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES," are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.

The draft SAR, which included criteria for retiring or modifying requirements, defined phases for the project, and a suggested list of requirements put together by NERC, the regions, and the trades and their member companies for consideration in Phase I, was posted for an informal comment period. In September, the P81 SDT met to respond to the comments received and finalize the SAR. The revisions resulted in a list of 38 requirements in 22 Reliability Standard versions being proposed for retirement and an additional 13 requirements included for informational purposes only. The P81 SDT also developed a Technical White Paper which includes the justification for retiring the proposed requirements.

To sign up for the plus list for this project to follow along with meetings and work products, please email Kristin Iwanechko.

Standards Development Process

The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-02 Paragraph 81

Recirculation Ballot Results

Now Available

A recirculation ballot window for the 20 standards with 36 requirements being proposed for retirement in this project concluded at **8 p.m. Eastern on Thursday, January 17, 2013**.

Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results.

Approval
Quorum: 84.60% Approval: 95.22%

Next Steps

The requirements being proposed for retirement will be presented to the Board of Trustees for retirement and then filed with the appropriate regulatory authorities.

Background

On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated the following in P81:

> "The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC,

the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

The purpose of the project is to retire or modify FERC-approved Reliability Standard requirements that as FERC noted, "provide little protection to the reliable operations of the BES," are redundant or unnecessary, or to retire or modify a FERC-approved Reliability Standard requirement to increase the efficiency of the ERO's compliance programs.

The draft SAR, which included criteria for retiring or modifying requirements, defined phases for the project, and a suggested list of requirements put together by NERC, the regions, and the trades and their member companies for consideration in Phase I, was posted for an informal comment period. In September, the P81 SDT met to respond to the comments received and finalize the SAR. The revisions resulted in a list of 38 requirements in 22 Reliability Standard versions being proposed for retirement and an additional 13 requirements included for informational purposes only. The P81 SDT also developed a Technical White Paper which includes the justification for retiring the proposed requirements.

After considering stakeholder comments from the formal comment period and initial ballot that ended on December 10, 2012, the drafting team moved CIP-001-2a R4 and EOP-004-1 R1 to the 'Informational Purposes Only' section in the technical paper, as EOP-004-2 has been filed with regulatory authorities and the EOP-004-2 implementation plan calls for the retirement of CIP-001-2a R4 and EOP-004-1 R1. This resulted in a final list of 36 requirements in 20 Reliability Standard versions.

To sign up for the plus list for this project to follow along with meetings and work products, please email Kristin Iwanechko.

Standards Development Process

The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results

Ballot Name:	Project 2013-02 Recirculation Ballot
Ballot Period:	1/8/2013 - 1/17/2013
Ballot Type:	Recirculation
Total # Votes:	357
Total Ballot Pool:	422
Quorum:	**84.60 % The Quorum has been reached**
Weighted Segment Vote:	95.22 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	112	1	89	0.967	3	0.033	3	17
2 - Segment 2.	10	1	9	0.9	1	0.1	0	0
3 - Segment 3.	98	1	79	0.988	1	0.013	2	16
4 - Segment 4.	37	1	25	1	0	0	2	10
5 - Segment 5.	95	1	77	0.987	1	0.013	2	15
6 - Segment 6.	51	1	46	1	0	0	0	5
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	9	0.8	7	0.7	1	0.1	0	1
9 - Segment 9.	3	0.1	1	0.1	0	0	2	0
10 - Segment 10.	7	0.6	5	0.5	1	0.1	0	1
Totals	**422**	**7.5**	**338**	**7.142**	**8**	**0.359**	**11**	**65**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1		Vijay Sankar		
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Abstain	
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Negative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Long Island Power Authority	Robert Ganley		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees		
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	National Rural Electric Cooperative Association	Paul McCurley	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	

1	Omaha Public Power District	Doug Peterchuck		
1	Oncor Electric Delivery	Jen Fiegel		
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County, Washington	Rod Noteboom		
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik		
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Steven Norris	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Robert Lafferty	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Buckeye Power, Inc.	Patrick O'Loughlin	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Hudson Gas & Electric Corp.	Thomas C Duffy	Negative	

3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Homestead	Orestes J Garcia	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City of Ukiah	Colin Murphey	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	Richard Blumenstock	Abstain	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr		
3	East Kentucky Power Coop.	Patrick Woods	Affirmative	
3	Entergy	Joel T Plessinger		
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Danny Lindsey	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed		
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage		
3	Municipal Electric Authority of Georgia	Steven M. Jackson		
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Gary Clear		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	

3	Puget Sound Energy, Inc.	Erin Apperson		
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott		
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alabama Municipal Electric Authority	Raymond Phillips		
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Buckeye Power, Inc.	Manmohan K Sachdeva	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	
4	Consumers Energy	David Frank Ronk	Abstain	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	LaGen	Richard Comeaux		
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Turlock Irrigation District	Steven C Hill		
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	

5	Bridgeport Energy	Cleyton Tewksbury		
5	Buckeye Power, Inc.	Paul M Jackson	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Grand Island	Jeff Mead	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative	
5	Colorado Springs Utilities	Jennifer Eckels		
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Abstain	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	East Kentucky Power Coop.	Stephen Ricker	Affirmative	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer		
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Essential Power, LLC	Patrick Brown	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	ExxonMobil Research and Engineering	Martin Kaufman	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego		
5	MidAmerican Energy Co.	Neil D Hammer	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Laurel Heacock		
5	Oklahoma Gas and Electric Co.	Kim Morphis	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	Colin Anderson	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	PacifiCorp	Bonnie Marino-Blair	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Abstain	

5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Affirmative	
5	Southern California Edison Company	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	Modesto Irrigation District	James McFall		
6	Muscatine Power & Water	John Stolley	Affirmative	
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried		
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Kelly Cumiskey	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Ty Bettis	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	

6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Abstain	
9	New York State Department of Public Service	Thomas G. Dvorsky	Abstain	
10	Midwest Reliability Organization	William S Smith		
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	

Exhibit G

Team Roster for NERC Standards Development Project 2013-02

Project 2013-02 Paragraph 81

Name and Title	Company and Address	Contact Info	Bio
Brian J. Murphy, Chair Manager, NERC Reliability Standards	NextEra Energy, Inc. 4200 W. Flagler Street Miami, FL 33134	(305) 442-5132 Brian.J.Murphy@fpl.com	Brian Murphy has worked for NextEra for over 12 years. Most recently, he was the primary drafter of NextEra Energy's NERC Reliability Standards Compliance Plan, including templates related to processes, controls and the overall supervision of compliance. Worked with Subject Matter Experts (SMEs) on compliance with all mandatory Reliability Standards issues during internal self assessments, spot checks as well as external spot checks and compliance audits. Worked with SMEs on policy and technical comments related to SARs, proposed and revised Reliability Standards, etc. Chair of NERC Standards Committee. Provide support to NextEra SMEs who participate on NERC standard drafting teams. Worked for eight years in Florida Power & Light Company's Transmission Department; and, worked closely with field and construction engineers, transmission planners and system operations on interconnection agreements, procedures, network issues, the sale of transmission, and Open Access Transmission Tariff (OATT) and Standards of Conduct issues. Drafted and negotiated a variety of transmission-related agreements. Field supervisor for contractor distribution crews during hurricane restoration. Significant training and experience in dispute resolution/facilitation, including the recent successful conducting a dispute resolution process that involved over 40 employees. Based on variety of training, Brian lead a pilot program to enhance skillful listening and communications, emotional intelligence, mindfulness and team work. As well, worked closely with Trade Associations, NERC and NERC regions on draft SAR and potential list of requirements for withdrawal. Prior to joining NextEra Energy, DTE Energy's liaison with FERC on technical and policy matters. Also, significant experience, while in private legal practice in Washington, D.C., drafting regulatory regulations, orders (including summarizing and responding to parties positions) and rules for governmental clients (including technical electric utility regulations), as well as chairing electric and gas utility working groups for governmental client and significant amount of project management experience. Holds a Bachelor's of Arts from Siena College and Juris Doctorate from University of Detroit School of Law.

Guy Zito, Vice Chair Assistant Vice President-Standards	Northeast Power Coordinating Council 1040 Avenue of the Americas, 10th Floor New York, NY 10018	(212) 840-1070 gzito@npcc.org	Guy Zito has been with Northeast Power Coordinating Council (NPCC) for in excess of 13 years. The last seven years he has worked as the Assistant Vice President of Standards and in that role developed the standards development process for the NPCC region as well as all the associated processes. He chairs a Regional Standards Committee that evaluates all standard projects and coordinates subject matter expert reviews of those standards. He participates in commenting and develops ballot recommendations for those standards to the entities in the northeast. He participates in various NERC standards activities such as the Standards Committee and its Process Subcommittee, and the Functional Model Working Group and has developed such initiatives for NERC as the Cost Effective Analysis Process or CEAP. The first six years with NPCC were served as the Manager of Planning with support given to regional groups of system studies engineers and also system planning engineers. Mr. Zito led a team of engineers to study constrained transmission in the northeast and how generators affected those constraints. He also manages the NPCC IT Dept. on a day to day basis and maintains responsibility for the reliability, effective, and efficient use of NPCC's IT resources. Also he is responsible for the IT Policies and Procedures for the region. Prior to joining NPCC, he was acting Director of Transmission Services at United Illuminating an investor owned utility, where he conducted and directed planning studies, interconnection studies, rate development and siting. Also in his role he was responsible for filings with the FERC, operations and also principle participant in ISO New England/NEPOOL activities pertaining to markets, planning, studies, and operation. He also was involved in various transmission major projects and the divestiture of generation assets. Prior to directing transmission services, he was Lead Customer Engineer in distribution. Duties included design of distribution to feed major customers using switchgear, underground vaults, distribution network systems, as well as overhead pole lines. He also ran numerous multimillion dollar state projects involving road widening and designed ductline systems in bridges. He supervised construction of large distribution projects and has extensive experience in project management. Mr. Zito has a BSEE from the University of New Haven, and an advance power engineering certificate from Power Technologies Incorporated.

Michael Brytowski Standards Specialist	Great River Energy 12300 Elm Creek Boulevard Maple Grove, MN 55369	(763) 445-5961 mbrytowski@grenergy.com	Michael Brytowski has been involved with the Electric Utility Industry for 25 years and is currently employed with Great River Energy as their NERC Standards Specialist. Previously, Michael worked at the Midwest Reliability Organization (MRO) as a NERC Compliance Auditor from March 2009 through March 2011 and as a Standards Specialist and secretary of the NSRS from February 2007 through June 2009. As Standards Specialist, Michael was Secretary of the MRO Augmentations drafting team, participated on the NERC VSL and NERC EOP VSL drafting teams, and participated in the development of the MRO Reliability Standards Voting Process (RSVP) application. Michael participated in the early development of the NERC Critical Infrastructure Protection Working Group/Committee from June 2000 through December 2001. Michael was a Reliability Coordinator at the Mid-Continent Area Power Pool (MAPP) for twelve years.
Doug Johnson Compliance Manager	American Transmission Company, LLC W234 N2000 Ridgeview Parkway Court Waukesha, WI 53188	(262) 506-6863 dfjohnson@atcllc.com	Doug Johnson has 34 years of combined experience in the electric transmission and nuclear power generating industries. Mr. Johnson has served as the Manager of Operational Compliance at American Transmission Company LLC since 2006. In his current role, Mr. Johnson is responsible for managing corporate programs for assuring compliance with NERC and FERC reliability regulations applicable to the electric transmission business. From 2000 to 2006, Mr. Johnson served as the Director of Regulatory Affairs and Strategic Issues for Nuclear Management Company. In this capacity, Mr. Johnson was responsible for directing the staffs at Nuclear Management Company's fleet of nuclear power plants which had responsibility for compliance, licensing, regulatory affairs, license renewal, corrective action program, risk assessment, environmental assessments, and root cause analyses. Mr. Johnson served as Nuclear Management Company's primary interface with staff at the Nuclear Regulatory Commission. He was also responsible for working with industry counterparts and industry trade and lobbying organizations to assure the promulgation of effective federal regulations which assured the safe and reliable operation of the country's nuclear generating assets. From 1980 to 2000, Mr. Johnson was employed by Wisconsin Electric Power Company and supported the operation of the Point Beach Nuclear Plant. He held varying responsibilities in the areas of nuclear compliance, licensing, regulatory affairs, operations, security, risk management and radiation safety. At the end of his tenure at Wisconsin Electric Power Company, Mr. Johnson was responsible for supporting the formulation of the business model for Nuclear Management Company and for coordinating the development and start-up of Nuclear Management Company with the executive teams at the five Midwestern utilities which contributed their nuclear generating assets to the Nuclear Management Company fleet. Mr. Johnson holds a Master of Business Administration from Marquette University and a Master of Science Degree in Nuclear Physics from the University of Pittsburgh.

David Kiguel Manager, Reliability Standards	Hydro One Networks, Inc. 483 Bay Street, TCT06 Toronto, Ontario M5G 2P5	(416) 345-5313 david.kiguel@hydroone.com	David Kiguel has been with Hydro One Networks Inc., and its predecessor, Ontario Hydro, for over 30 years. He currently holds the position of Manager-Reliability Standards. During most of his career he has worked in reliability modelling and assessments. For the past 10 years he has been involved in legal and regulatory issues in the evolving North American electricity industry as well as in the review of emerging reliability standards and their development processes. He also provides support in the reliability standards compliance activities within Hydro One Networks Inc. and in the overall Hydro One Internal Reliability Program and Framework. David has been a member of the NERC Standards Committee from 2008 to 2010 inclusive and again in 2012 and 2013. Also, he has been a member of the NERC Standards Committee Process Subcommittee for the past 6 years. In 2010 and 2012, he was elected by the SC members to be part of the Standards Committee Executive Committee. He is also an active participant in the Northeast Power Coordinating Council (NPCC) where he is a member of the Compliance Committee, the Regional Standards Committee (RSC) and the RSC Executive Committee. He also participates in the Compliance Practices Group of the North American Transmission Forum and in the Ontario IESO's Reliability Standards Standing Committee. Mr. Kiguel is a registered professional engineer in Professional Engineers Ontario (PEO), where he is a member of the Experience Requirements Committee. He is an IEEE Senior Member.
Scott Kinney Director, System Operations	Avista Corporation P.O. Box 3727 Spokane, WA 99220	(509) 495-4494 scott.kinney@avistacorp.com	Scott is responsible for managing the System Operations Department at Avista, which includes the Transmission control center (TOP/BA functions), the EMS/SCADA department (CIP standards), Transmission Planning (TPL functions), Transmission Contracts and Services including OASIS (MOD standards) and Distribution Dispatch control center. Scott is the incoming Vice-chair of the WECC Operating Committee. He is an active member in WECC operating efforts including a past member of the WECC Operating Transfer Capability Policy Committee which approved WECC seasonal SOLs, a member of the WECC Compliance Hearing Body, and is the WECC Avista Member representative. He just completed a two year term as the Chair of both the Northwest Power Pool Operating Committee and the Reserve Sharing Group Committee. He currently sits on the Steering Committee for Columbia Grid, the FERC approved regional Planning and Operating entity. Scott actively participates on the EEI Reliability Executive Advisory Committee. Scott has managed the System Operations Department at Avista for over 11 years, has 13 years of technical operations experience and 8 years of transmission planning experience.

Kevin Koloini Director of Reliability Standards Compliance	American Municipal Power, Inc. 1111 Schrock Road Suite 100 Columbus, OH 43229	(614) 540-0857 kkoloini@amppartners.org	Mr. Koloini is responsible for NERC reliability standards compliance and communicating reliability standards compliance requirements to applicable departments, staff and municipal organizations. He works with internal subject matter experts to develop policies and procedures to comply with reliability standards. He monitors AMP departments for compliance and reports status to senior management and the board of trustees. He coordinates AMP and member interests on reliability issues and standards development. In his previous roles, Kevin has worked on many engineering projects in distribution, generation, energy efficiency and smart grid research. He has also been heavily involved in forecasting, planning, project management, billing, rates, contracts and regulatory compliance. Kevin has worked directly with over 60 companies that have been registered with NERC as Distribution Providers, Load Serving Entities, Purchasing and Selling Entities, Resource Planners, Generator Owners, and Generator Operators and has assisted 22 with audit preparation. Kevin has just completed a two-year term representing the Transmission Dependent Utilities sector on the North American Electric Reliability Corporation Planning Committee, is a member of the RFC/SERC Small Entity Working Group, and is a member of the North American Generator Forum. He also works closely with the Transmission Access Policy Study Group and the American Public Power Association. Kevin received a Bachelor of Science from Ohio State University in Electrical and Computer Engineering, a Distribution Engineering Certificate from the University of Wisconsin at Madison, and a Business Leadership Certificate from Cornell University. Kevin is a certified Project Management Professional.

Mark Ladrow Senior Compliance Assessment Engineer	SERC Reliability Corporation 2815 Coliseum Centre Drive Suite 500 Charlotte, NC 28217	(704) 940-8217 mladrow@serc1.org	Mark Ladrow joined SERC Reliability Corporation in 2007, and is currently a Senior Compliance Assessment Engineer. He is a member of the Compliance Programs staff with responsibilities including entity Compliance Assessments and Compliance Investigations. Previously, Mr. Ladrow was the Manager of Reliability Standards for the North American Electric Reliability Council (NERC) in Princeton, NJ where he managed the ANSI accredited standards process for electric grid reliability. Reporting directly to Gerry Cauley, he was responsible for the content of new and modified Reliability Standards ensuring that they are clear, concise, and enforceable. He served as the primary contact to stakeholders for all Reliability Standard issues, represented NERC at various industry and regulatory venues, and was a key interface in a team effort alongside leading industry professionals in the development of the Electric Reliability Standards supporting the overall mission of a safe and reliable electric grid for North America. Over the course of 24 years in the electric power industry, Mark has held several key management positions. Mr. Ladrow served as the Assistant Vice President for Power Products ACE USA in Philadelphia, PA where he worked in sales and marketing of insurance-based, market settled risk products to the regulated and non-regulated electric industry. As Manager of Energy Marketing of Trigen Energy Group, Mark negotiated wholesale off-take agreements for surplus energy from cogeneration projects located throughout contiguous U.S. He also provided recommendations on the viability of oversized cogeneration projects based on research of regulatory and market environments. Serving as Manager of Power Supply for The United Illuminating Company, Mark managed short-term power supply for a 1200 MW portfolio of regulated assets, optimizing the daily and monthly generation portfolio to maximize the value to shareholders. He sat as a voting member or alternate member on several NEPOOL subcommittees. Mr. Ladrow holds an MBA from Southern New Hampshire University, Manchester, NH and a BS, Mechanical Engineering from the University of Bridgeport, Bridgeport, CT.

Scott McGough Bulk Electric System Compliance Manager	Georgia System Operations Corporation 2100 East Exchange Place Tucker, GA 30084	(770) 270-7689 scott.mcgough@gasoc.com	Scott McGough has more than 7 years electric industry experience as a program manager developing and implementing compliance programs. He pioneered Oglethorpe Power Corporation's (OPC) GO and GOP compliance program. At OPC, his responsibilities included reviewing new reliability standards and applying compliance-related policies and procedures into OPC's program; assessing compliance and operational risk and conducting reliability audits. He managed the AURORA cyber vulnerability project while working with NRECA representatives and played a strategic role in discussions with FERC regarding this initiative. Also, Scott worked closely with Trade Associations, NERC and NERC regions on developing the draft SAR and potential list of requirements for withdrawal. Scott recently moved to Georgia System Operations Corporation's (GSOC) Compliance Department where he directs program enhancements for the TOP and LSE related compliance activities. He is currently GSOC's FERC 693 compliance manager and serves a support role in GSOC's CIP compliance program. Scott holds a Bachelor of Science degree from Oklahoma State University.
Ken McIntyre Director Standards and Protocols Compliance	Electric Reliability Council of Texas, Inc. 2705 West Lake Drive Taylor, TX 76574	(512) 248-3969 kmcintyre@ercot.com	Ken McIntyre received his Bachelors of Electrical/Electronic Engineering from the University of Southern Queensland, Australia, and Master of Business from Charles Sturt University, Australia. He has seventeen years of power industry experience, including working in the Australian power industry from 1995 to 2006, before joining the Electric Reliability Council of Texas (ERCOT) in 2007. Ken commenced work with the Queensland Electricity Commission in 1995, before moving to Powerlink Queensland upon the deregulation of the electricity industry and the introduction of the National Electricity Market. At Powerlink Queensland, Ken worked in both transmission and substation engineering, before moving into power system operations. During his time in operations, Ken was an accredited Transmission System Operator before becoming the Lead for Operations Planning, Real-time Support and Outage Coordination. Since working for ERCOT, Ken has held the positions of Senior Operations Planning Engineer, Supervisor of Advanced Network Applications and Manager of Operations and Planning Standards, before his recent promotion as the Director Standards and Protocols Compliance. In this current role, Ken is responsible for ERCOT meeting its regulatory responsibilities for both the NERC Reliability Standards and the ERCOT Protocols and Operating Guides, and to provide guidance to and increased reliability assurance for, the ERCOT region. Ken has been a member of a standards drafting team, invited to NERC Focus Groups, and presented at FERC Technical Conference. He is also a proxy member of the NERC Certification and Compliance Committee (CCC).

Stephanie Monzon Manager of NERC and Regional Coordination	PJM Interconnection, LLC 944 Jefferson Avenue Norristown, PA 19403	(610) 666-8870 monzos@pjm.com	Stephanie Monzon is a mechanical engineer with over 12 years experience in the industry. Prior to PJM, Stephanie was a Manager at NERC within the Standards group focused on Regional Standards. She also coordinated several drafting teams. Prior to NERC, she worked for PJM in various roles including senior engineer in Operations, AC2 (Second Control Center Project), and the NERC and Regional Coordination group. In her current role Stephanie is the Manager of NERC and Regional Coordination for PJM. She is responsible for overseeing the 693 Compliance program and for coordinating NERC activities. She is also a member of the Paragraph 81 team and has worked closely with Trade Associations, NERC and NERC regions on developing the draft SAR and potential list of requirements for withdrawal.
Stephen Pelcher Deputy General Counsel Nuclear and Regulatory Compliance	South Carolina Public Service Authority (Santee Cooper) One Riverwood Drive Moncks Corner, SC 29461	(843) 761-4016 stephen.pelcher@santeecooper.com	Steve's current responsibilities at Santee Cooper include providing ongoing legal advice concerning compliance issues associated with the NERC Reliability Standards. Steve has worked closely with Trade Associations, NERC and NERC regions on developing the draft SAR and potential list of requirements for withdrawal.
Mark A. Pratt Reliability Standards Compliance Assurance Manager	Southern Company 600 North 18th Street Birmingham, AL 35203	(205) 257-7670 mapratt@southernco.com	At Southern Company, Mark is responsible for managing compliance activities and programs that support reliability standards compliance in all functional areas for Southern Company Operations over three Regions (SERC, FRCC and Texas RE). Mark has actively participated in every reliability standards audit of Southern Company since 2007. Also, Mark worked closely with Trade Associations, NERC and NERC regions on developing the draft SAR and potential list of requirements for withdrawal. Prior to this role, Mark served as the Data & Compliance Manager in Southern Company's Fleet Operations and Trading organization with a focus on, among other things, the reliability standards applicable to the GO, GOP and PSE functions. Mark has a total of 25 years experience in the electric utility industry including 16 years in fossil and nuclear power plant operations, maintenance and engineering with Southern Company, Florida Power Corporation (Now Duke/Progress Energy Florida) and Bechtel Power Corporation. Mark is a registered Professional Engineer in the state of Florida and holds a bachelors degree in nuclear engineering from the University of Florida and a masters degree in mechanical engineering from the University of South Florida.
Frank Vick Compliance Team Lead	Texas Reliability Entity, Inc. 805 Las Cimas Parkway, Suite 200 Austin, TX 78746	(512) 583-4949 frank.vick@texasre.org	As an Auditor and Compliance Team Lead for Texas RE since 2005, Frank Vick has actively participated in the NERC Compliance Monitoring Processes Working Group. Frank was a contractor for CenterPoint Energy from 1997 through 2005. Frank previously spent over 20 years at CenterPoint Energy (1974 –1996) in their Electrical Systems and Substation Engineering Divisions supporting relaying, planning, and major equipment procurement functions.

Mary Ann Zehr Senior Transmission Policy Specialist-Transmission Contracts, Rates, and Policy	Tri-State Generation and Transmission Association, Inc. 1100 W. 116th Avenue Westminster, CO 80234	(303) 254-3098 mzehr@tristategt.org	Mary Ann Zehr has twelve years of experience in the energy industry, currently holding the position of Senior Transmission Policy Specialist for Tri-State Generation and Transmission Association, Inc. Tri-State is a wholesale electric power supplier owned by the 44 electric cooperatives that it serves. Tri-State generates and transmits electricity to its member systems throughout a 200,000 square-mile service territory across Colorado, Nebraska, New Mexico and Wyoming, serving approximately 1.5 million customers. Mary Ann's current position as Senior Transmission Policy Specialist affords her the opportunity to frequently engage in the review and analysis of current and proposed NERC and WECC reliability standards as well as monitor Tri-State's adherence to and compliance with those standards. Preceding her transition to transmission policy, Mary Ann spent several years as a NERC Certified (RC) System Operator. Prior to joining Tri-State, Mary Ann served in the U.S. Navy as a nuclear power plant operator for six years. Mary Ann's educational background includes a Master's of Science Degree in Global Energy Management from the University of Colorado which included research in various facets of U.S. and Foreign Energy Policy and a Bachelor's of Science Degree in Business Administration with a specialization in Management from Regis University.